McAfee Content Security Blade Server

Installationshandbuch

COPYRIGHT

Copyright © 2011 McAfee, Inc. Alle Rechte vorbehalten.

Diese Publikation darf in keiner Form und in keiner Weise ohne die schriftliche Genehmigung von McAfee, Inc., oder ihren Lieferanten und angeschlossenen Unternehmen ganz oder teilweise reproduziert, übermittelt, übertragen, in einem Abrufsystem gespeichert oder in eine andere Sprache übersetzt werden.

MARKEN

AVERT, EPO, EPOLICY ORCHESTRATOR, FOUNDSTONE, GROUPSHIELD, INTRUSHIELD, LINUXSHIELD, MAX (MCAFEE SECURITYALLIANCE EXCHANGE), MCAFEE, NETSHIELD, PORTALSHIELD, PREVENTSYS, SECURITYALLIANCE, SITEADVISOR, TOTAL PROTECTION, VIRUSSCAN, WEBSHIELD sind eingetragene Marken oder Marken von McAfee, Inc. und/oder der Tochterunternehmen in den USA und/oder anderen Ländern. Die Farbe Rot in Verbindung mit Sicherheit ist ein Merkmal der McAfee-Produkte. Alle anderen eingetragenen und nicht eingetragenen Marken in diesem Dokument sind alleiniges Eigentum der jeweiligen Besitzer.

INFORMATIONEN ZUR LIZENZ

Lizenzvereinbarung

HINWEIS FÜR ALLE BENUTZER: LESEN SIE DEN LIZENZVERTRAG FÜR DIE VON IHNEN ERWORBENE SOFTWARE SORGFÄLTIG DURCH. ER ENTHÄLT DIE ALLGEMEINEN BESTIMMUNGEN UND BEDINGUNGEN FÜR DIE VERWENDUNG DER LIZENZIERTEN SOFTWARE. WENN SIE NICHT WISSEN, WELCHEN SOFTWARE-LIZENZTYP SIE ERWORBEN HABEN, SCHLAGEN SIE IN DEN UNTERLAGEN ZUM KAUF UND WEITEREN UNTERLAGEN BEZÜGLICH DER LIZENZGEWÄHRUNG ODER DEN BESTELLUNTERLAGEN NACH, DIE SIE ZUSAMMEN MIT DEM SOFTWAREPAKET ODER SEPARAT (ALS BROSCHÜRE, DATEI AUF DER PRODUKT-CD ODER ALS DATEI, DIE AUF DER WEBSITE VERFÜGBAR IST, VON DER SIE AUCH DAS SOFTWAREPAKET HERUNTERGELADEN HABEN) ERHALTEN HABEN. WENN SIE MIT DEN IN DIESER VEREINBARUNG AUFGEFÜHRTEN BESTIMMUNGEN NICHT EINVERSTANDEN SIND, UNTERLASSEN SIE DIE INSTALLATION DER SOFTWARE. SOFERN MÖGLICH, GEBEN SIE DAS PRODUKT AN MCAFEE ODER IHREN HÄNDLER BEI VOLLER RÜCKERSTATTUNG DES KAUFPREISES ZURÜCK.

Inhaltsverzeichnis

Einführung in McAfee Content Security Blade Server 7

Verwendung dieses Handbuchs 7

Zielgruppe dieses Handbuchs 7

Definition der Begriffe in diesem Handbuch 8

Graphische Konventionen 9

Dokumentation 9

Verfügbare Ressourcen 9

Einführung in Blade-Server 11

Hauptvorteile der Blade-Server 11

Typen von Blades 12

Management-Blade-Server 13

Failover-Management-Blade-Server 13

Blade-Server zum Scannen von Inhalten 13

Vorbereitung der Installation 15

Lieferumfang 15

Planen der Installation 16

Unangemessene Nutzung 16

Platzieren des Blade-Servers 16

Überlegungen zu Netzwerkmodi 17

Modus "Transparente Bridge" 17

Modus "Transparenter Router" 20

Modus "Expliziter Proxy" 21

Ausbringungsstrategien für die Verwendung des Geräts in einer DMZ 23

SMTP-Konfiguration in einer DMZ 24

Arbeitslastverwaltung 26

Integrierte Redundanz 26

Planen der Installation 27

Vor dem Start einer Standardinstallation 27

Vor dem Installieren des Gehäuses 28

Einrichten der Lights-Out-Verwaltung 30

Nach der Installation 30

Anschließen und Konfigurieren des Blade-Servers 31

Upgrades von früheren Versionen 31

Konfigurieren der Interconnect-Module bei der Aktualisierung von einer älteren Version 32

Sichern der vorhandenen Konfiguration 33

Herunterfahren der Scan-Blades 33

Herunterfahren der Management-Blade-Server 34

Upgrade der Software für den Management-Blade-Server 34

Erneute Installation der Scan-Blades 35

Standardinstallation 36

Montieren des Blade-Servers 37

Installieren der Interconnect-Module 38

Anschließen des Blade-Servers an das Stromnetz 39

Verbindung mit dem Netzwerk 40

Installieren der Software 42

Installationsreihenfolge der Management-Blade-Server 42

Software-Images 42

Installieren der Software auf einem Blade-Server zum Scannen von Inhalten 44

Verwenden der Konfigurationskonsole 44

Begrüßungsseite 45

Durchführen der benutzerdefinierten Einrichtung 45

Wiederherstellung aus einer Datei 52

Erste Schritte mit dem Content Security Blade Server 53

Die Benutzeroberfläche 53

Dashboard-Statusinformationen und Konfigurationsoptionen 55

Funktionen des Blade-Servers 60

Demonstrieren der Failover- und Arbeitslastverwaltung 60

Testen der Verwaltungsfunktionen auf dem Blade-Server 61

Verwenden von Richtlinien für die Verwaltung von Nachrichten-Scans 63

Testen der Konfiguration 68

Testen der Verbindung 68

Aktualisieren der DAT-Dateien 68

Testen von E-Mail-Verkehr und Virenerkennung 69

Testen der Spam-Erkennung 69

Testen von Web-Verkehr und Virenerkennung 69

Funktionen des Content Security Blade Servers 70

Scan-Richtlinien und deren Einfluss auf Ihr Netzwerk 70

Inhaltsscans unter Verwendung der E-Mail-Compliance-Regeln 70

Vermeiden des Verlusts vertraulicher Daten. 72
Bearbeiten von isolierten Nachrichten. 73
Überwachen der Spam-Erkennung. 73
Überwachen der Web-Aktivität. 74

Betrieb im ausfallsicheren Modus **75**

Nutzung der Hardware im ausfallsicheren Modus. 75
Entscheidung treffen zur Verwendung des ausfallsicheren Modus. 77
Vor dem Umkonfigurieren in den ausfallsicheren Modus. 77
Hardware-Informationen. 77
Benutzernamen und Kennwörter. 78
Aktivieren des ausfallsicheren Modus. 79
Sichern der vorhandenen Konfiguration. 80
Installieren der Interconnect-Module für den ausfallsicheren Modus. 80
Konfigurieren der Interconnect-Module. 83
Ändern der Gehäusekonfiguration. 85
Konfigurieren des Management-Blade-Servers für die Verwendung des ausfallsicheren Modus. 88
Verbindungen zum externen Netzwerk im ausfallsicheren Modus. 88
Einschalten der Blades. 90

Fehlerbehebung **91**

Blade-spezifische Fehlerbehebung. 91
Externe Überwachungssysteme. 91
Status der Netzwerkkarte. 92
Systemereignisse. 92
Systemkonfiguration. 92
Transparente Web-Authentifizierung. 92
Anti-Spam. 93
Automatische Aktualisierung der Antiviren-Software. 95
Zustellung. 96
Die Directory Harvest-Prävention funktioniert nicht. 96
E-Mail-Anhänge. 96
ICAP. 97
E-Mail-Probleme. 99
POP3. 100
Allgemeine Probleme. 100
Systemverwaltung. 101
Weitere Hilfe – Die Link-Leiste. 101

Anhänge **102**

Beispiel für die Basiskonfiguration eines Interconnect-Moduls 102

Beispiel einer Chassis-Konfigurationsdatei 103

Prozeduren für den Hardwareaustausch 106

Ersetzen eines ausgefallenen Scan-Blades 106

Ersetzen eines ausgefallenen Management-Blade-Servers 107

Ersetzen eines ausgefallenen Failover-Management-Blade-Servers 107

Ersetzen eines ausgefallenen Interconnect-Moduls 107

Ersetzen eines ausgefallenen Onboard-Administrator-Moduls 108

Einführung in McAfee Content Security Blade Server

In diesem Handbuch erhalten Sie die notwendigen Informationen für die Installation der Software für McAfee® Content Security Blade Server Version 5.6, die mit dem M3- und M7-Blade-Server-Chassis ausgeliefert wird. Es erläutert die Schritte und die Verifikation des Installationsprozesses.

HINWEIS: Die Begriffe *Chassis* und *Gehäuse* werden in der Dokumentation synonym verwendet.

In diesem Handbuch wird beschrieben, wie Sie Content Security Blade Server 5.6 installieren und konfigurieren. Nach Abschluss haben Sie einen vollständig funktionsfähigen Server.

Inhalt

- Verwendung dieses Handbuchs
- Definition der Begriffe in diesem Handbuch
- Graphische Konventionen
- Dokumentation

Verwendung dieses Handbuchs

In diesem Handbuch wird Folgendes behandelt:

- Planung und Ausführung Ihrer Installation.
- Umgang mit der Benutzeroberfläche.
- Testen der ordnungsgemäßen Funktion des Produkts.
- Anwendung der aktuellsten Erkennungsdefinitionsdateien.
- Vertrautmachen mit einigen Scan-Richtlinien, Erstellen von Berichten und Abrufen der Statusinformationen.
- Beheben einiger grundlegender Probleme.

Weitere Informationen zu den Scan-Funktionen des Produkts finden Sie in der Online-Hilfe.

Zielgruppe dieses Handbuchs

Dieses Handbuch richtet sich in erster Linie an Netzwerkadministratoren, die für das Virenschutz- und Sicherheitsprogramm ihres Unternehmens verantwortlich sind.

Definition der Begriffe in diesem Handbuch

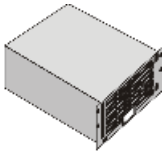
In diesen Informationen werden einige der in diesem Handbuch häufig verwendeten Begriffe definiert.

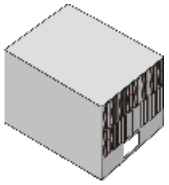
Begriff	Beschreibung
Demilitarisierte Zone (DMZ)	Ein Computer-Host oder kleineres Netzwerk, das als Puffer zwischen ein privates Netzwerk und das äußere öffentliche Netzwerk eingefügt wurde, um den direkten Zugriff durch außenstehende Benutzer auf Ressourcen im privaten Netzwerk zu verhindern.
DAT-Dateien	Erkennungsdefinitionsdateien (DAT), auch als Signaturdateien bezeichnet, enthalten die Definitionen, die Viren, Trojaner, Spyware, Adware und andere potenziell unerwünschte Programme (PUPe) identifizieren, erkennen und entfernen.
Betriebsmodus	Es gibt drei Betriebsmodi für das Produkt: "Expliziter Proxy", "Transparente Bridge" und "Transparenter Router".
Richtlinie	Eine Sammlung der Sicherheitskriterien (z. B. Konfigurationseinstellungen, Benchmarks und Spezifikationen für den Netzwerkzugriff), die die erforderliche Compliance-Stufe für Benutzer, Geräte und Systeme definieren, die von einer McAfee-Sicherheitsanwendung bewertet oder erzwungen werden kann.
Reputationsdienst-Prüfung	Teil der Absenderauthentifizierung. Wenn ein Absender die Reputationsdienst-Prüfung nicht besteht, ist die Appliance so eingestellt, dass die Verbindung beendet und die Nachricht nicht zugelassen wird. Die IP-Adresse des Absenders wird zu einer Liste blockierter Verbindungen hinzugefügt und in Zukunft automatisch auf Kernel-Ebene blockiert.
OA (Onboard Administrator)	Die Module für die Verwaltung des gesamten HP-Blade-Chassis. Um den ausfallsicheren Betrieb zu gewährleisten, können in ein einzelnes Chassis zwei Modules eingebaut werden.
Interconnect-Modul	Die Bezeichnung für die Netzwerk-Switches, die sich im Blade-Chassis zwischen den Blade-Geräten und der externen Infrastruktur befinden.
Querverbindung	Die Bezeichnung für die internen Verbindungen zwischen den Interconnect-Modul-Fächerpaaren 1 und 2, 3 und 4, 5 und 6 sowie 7 und 8. Diese werden verwendet, um innerhalb des Chassis Ausfallsicherheit zu gewährleisten. Zwischen jedem Paar von Interconnect-Modul-Fächern gibt es zwei Querverbindungen, die üblicherweise gebündelt betrieben werden.
STP (Spanning Tree-Protokoll)	Ein Standardprotokoll, das verwendet wird, um Schleifen in Broadcast-Netzwerken zu vermeiden, und das redundante Pfade zulässt.
PVST (Per VLAN Spanning Tree)	Eine Cisco-eigene Erweiterung des STP, bei der der Spanning Tree innerhalb einer Gruppe von VLANs betrieben wird, unabhängig von anderen VLANs, die auf denselben physischen Verbindungen laufen. Das Interconnect-Modul HP GbE2C unterstützt PVST.
MSTP (Multiple Spanning Tree-Protokoll)	Dies ist eine standardmäßige Erweiterung des STP, die es erlaubt, den Spanning Tree unabhängig von anderen VLAN-Gruppen zu betreiben.
iLO (Integriertes Lights-Out-Verwaltungsmodul)	Der Name für das Modul auf jedem Blade, das die Lights-Out-Verwaltung des Blades ermöglicht.
OOB (Out-of-Band-Verwaltung)	Die von der Email and Web Security-Software bereitgestellte Funktion, die es ermöglicht, die Email and Web Security-Software über eine separate Netzwerkschnittstelle zu verwalten. Ist diese Option aktiviert, kann das Email and Web Security-Verwaltungsportal von den Schnittstellen für den gescannten Datenverkehr abgeschottet werden.
PXE (Pre-boot eXecution Environment)	Die Möglichkeit, einen Computer über das Netzwerk zu starten, bevor ein Betriebssystem installiert ist.

Begriff	Beschreibung
Gebündelte Verbindungen (Auch bekannt als Trunking, aggregierte Verbindung, Etherchannel, Portchannel)	Eine Möglichkeit, zwei Netzwerkverbindungen wie eine einzige Verbindung zu behandeln, um Ausfallsicherheit für den Fall zu gewährleisten, dass eine Verbindung ausfällt, und (abhängig von der Konfiguration) um die Bandweite zu erhöhen.
VLAN (Virtual LAN)	Eine Möglichkeit, eine einzelne Netzwerkverbindung in verschiedene Netzwerke zu unterteilen. Wird im Standard IEEE 802.1Q definiert.

Graphische Konventionen

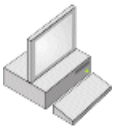
In den Abbildungen dieses Handbuches werden die folgenden Symbole verwendet.


Content Security Blade Server im M3-Gehäuse


Content Security Blade Server im M7-Gehäuse

E-Mail-Server

Internet


Benutzer- oder Client-Computer

Anderer Server (z. B. DNS-Server)

Switch

Router

Netzwerkzone (DMZ oder VLAN)

Firewall

Tatsächlicher Datenpfad

Netzwerk

Wahrgenommener Datenpfad

Dokumentation

Dieses Handbuch ist im Lieferumfang Ihres Produkts enthalten. Weitere Informationen finden Sie in der zum Produkt gehörenden Online-Hilfe und der weiteren Dokumentation auf der Website http://mysupport.mcafee.com.

Verfügbare Ressourcen

Hier wird beschrieben, wo Sie weitere Informationen und Hilfe erhalten können.

McAfee-Produkte	McAfee-KnowledgeBase. Gehen Sie zu https://mysupport.mcafee.com/eservice/Default.aspx,

	und klicken Sie auf **Search the KnowledgeBase** (KnowledgeBase durchsuchen).
Produkthandbuch	McAfee-Download-Site. Enthält Informationen zu grundlegenden Konzepten, Richtlinien, Protokollen (SMTP, POP3, FTP, HTTP und ICAP), zur Wartung und Überwachung. Sie benötigen Ihre Grant-Nummer.
Online-Hilfe	Produktoberfläche. Enthält Informationen zu grundlegenden Konzepten, Richtlinien, Protokollen (SMTP, POP3, FTP, HTTP und ICAP), zur Wartung und Überwachung.

Einführung in Blade-Server

Der McAfee® Content Security Blade Server Version 5.6 scannt Web- und E-Mail-Verkehr nach Viren, Spam und anderen Bedrohungen Ihres Netzwerks.

Die Blade-Server sind innerhalb der McAfee Email and Web Security-Produktpalette die Modelle mit der höchsten Kapazität.

Der Blade-Server:

- Scannt und verarbeitet Ihren SMTP- und POP3-Nachrichtenverkehr (Email Security-Software)
- Scannt und verarbeitet Ihren HTTP-, ICAP- und FTP-Verkehr (Web Security-Software)
- Läuft acht Mal schneller als eine eigenständige Email and Web Security Appliance.
- Reduziert die Raum- und Betriebskosten für Ihr Rechenzentrum gegenüber eigenständigen Appliances.
- Ist skalierbar. Sie können weitere Blade-Server zum Scannen von Inhalten hinzufügen, um den Scan-Durchsatz zu erhöhen, ohne die Leistung zu beeinträchtigen.
- Lässt sich einfach verwalten und bedienen. Verteilt die Scan-Arbeitslast gleichmäßig und aktualisiert die Erkennungsdefinitionsdateien (DAT) auf allen Blades.
- Kann die Software McAfee Web Gateway (vormals WebWasher) auf einigen oder allen Blade-Servern zum Scannen von Inhalten ausführen.

HINWEIS: Der Blade-Server verfügt über eine integrierte Arbeitslastverwaltung. Wenn Sie in Ihrem Netzwerk bereits einen Lastenausgleicher verwenden, können Sie diesen bei der Installation des Blade-Servers beibehalten, auch wenn er nicht mehr erforderlich ist, um die Scan-Arbeitslast gleichmäßig zu verteilen.

Inhalt

- Hauptvorteile der Blade-Server
- Typen von Blades

Hauptvorteile der Blade-Server

Schutz vor E-Mail-Bedrohungen

- Preisgekrönter Schutz vor E-Mail-Bedrohungen
- Erkennen und Blockieren von Spam, Phishing-Angriffe, Spyware und Viren, damit diese nicht in Ihre E-Mail-Systeme gelangen

Schutz vor Web-Bedrohungen

- Erkennen und Blockieren von Phishing-Websites, Spyware, potentiell unerwünschten Programme und Viren, damit diese nicht in Ihr Netzwerk heruntergeladen werden können

- Sie können die in der Software des Content Security Blade Server enthaltenen Web-Scan-Funktionen verwenden oder die Software McAfee Web Gateway (vormals WebWasher) auf einigen oder allen Blade-Servern zum Scannen von Inhalten installieren.
- Der preisgekrönte McAfee SiteAdvisor schützt Benutzer vor dem Besuch unangemessener Websites

Inhaltsfilterung

- Einhaltung von E-Mail-Datenschutzbestimmungen, beispielsweise den Health Insurance Portability and Accountability Act (HIPAA), den Sarbanes-Oxley Act (SOX), die Direktiven der Europäischen Union (EU), nationale Gesetze und weitere Regelungen.

Kostenersparnis

- Geringere Kosten für Produktkäufe sowie Lizenz- und Supportgebühren
- Geringere Rechenzentrumskosten für Kühlung, Platz und Energie
- Senkung von langfristigen Kapitalkosten

Hohes Maß an Durchsatz, Skalierbarkeit und Zuverlässigkeit

- Unterbrechungsfreier Kapazitätsausbau nach Bedarf durch Hot-Swap-fähige Blades
- Redundante Stromversorgung und automatisches Failover
- Modus für ausfallsicheren Betrieb, der besseren Schutz vor Netzwerkproblemen bietet, die das Scannen unterbrechen könnten

Bewährte Anti-Spam-Technologie

- Erkennen und Blockieren von mehr als 98 Prozent Spam, einschließlich der neuesten Bild-, PDF- und MP3-Spam-Attacken, ohne kritische Falsch-Positive (laut unabhängigen Tests)
- Streaming-Updates alle zwei bis drei Minuten, um neue Formen von Spam schnell abzuwehren
- Die hohe Wirksamkeit der Spamschutz-Funktion wird durch ein Zusammenspiel verschiedener Technologien erreicht, darunter:
  - McAfee® IP-Reputationsfilterung
  - Reputationsbewertung von Domänennamen
  - Heuristische Erkennung
  - Inhaltsfilterung
  - Absenderauthentifizierung auf der Grundlage der Standards Sender Policy Framework (SPF) und DomainKeys Identified Mail (DKIM)
  - Greylisting zur Verfolgung und Freigabe von Mails von bekannten, seriösen Absendern, während Mails von unbekannten Absendern vorläufig abgelehnt werden

Typen von Blades

In diesem Abschnitt werden die verschiedenen Blade-Typen beschrieben, die mit dem Blade-Server geliefert werden:

- Management-Blade-Server
- Failover-Management-Blade-Server

- Blade-Server zum Scannen von Inhalten

Management-Blade-Server

Der Management-Blade-Server verwaltet den Netzwerkverkehr und leitet den Verkehr mithilfe der integrierten Arbeitslastverwaltung an die Blade-Server zum Scannen von Inhalten weiter. Der Management-Blade-Server wird nicht zum Scannen von Dateien verwendet. Der Management-Blade-Server:

- Stellt die anfängliche Software-Installation für die Blade-Server zum Scannen von Inhalten zur Verfügung.
- Verwaltet alle Aktualisierungen für die anderen Blades.
- Aggregiert alle Ereignisse, isolierten E-Mails und zurückgestellten E-Mails.

Zu jeder Zeit ist entweder der Management-Blade-Server oder der Failover-Management-Blade-Server aktiv. Sie können nicht gleichzeitig aktiv sein.

Der Management-Blade-Server und die Blade-Server zum Scannen von Inhalten arbeiten wie ein einziges System zusammen, wenn Sie Folgendes tun:

- Konfigurationsänderungen mithilfe einer webbasierten Oberfläche vornehmen.
- Die DAT-Dateien aktualisieren.
- Statusinformationen anzeigen.

Der Management-Blade-Server stellt außerdem sicher, dass:

- Das gesamte System auch während Aktualisierungen in Betrieb ist.
- Aktualisierungen nicht durchgeführt werden, wenn eine vorhergehende Aktualisierung fehlgeschlagen ist.
- Relevante Warnungen (z. B. SNMP) erzeugt werden, wenn Blades hinzugefügt oder entfernt werden oder ausfallen.

Der Management-Blade-Server kann mit Folgendem interagieren:

- Mit den Blade-Servern zum Scannen von Inhalten, um einzelne Scan-Blades herunterzufahren, neu zu starten oder zu deaktivieren.
- Mit McAfee Quarantine Manager. Die Quarantine Manager-Anwendung gewährleistet, dass Ihr Netzwerk über eine zentralisierte Quarantäneressource verfügt.

Failover-Management-Blade-Server

Der Failover-Management-Blade-Server ist baugleich mit dem Management-Blade-Server. Er übernimmt die Verwaltungsfunktionen, falls der Management-Blade-Server ausfällt. Hierfür verwendet er:

- Spanning Tree-Protokoll (STP) für den Modus "Transparente Bridge".
- Virtual Router Redundancy Protocol (VRRP) für die Modi "Transparenter Router" und "Expliziter Proxy".

Der Failover-Management-Blade-Server wird nicht zum Scannen von Dateien verwendet. Sofern er konfiguriert ist, bleibt er inaktiv, bis er gebraucht wird.

Blade-Server zum Scannen von Inhalten

Mit dem Blade-Server wird mindestens ein Blade-Server zum Scannen von Inhalten ausgeliefert.

Wenn Sie zum ersten Mal einen Blade-Server zum Scannen von Inhalten installieren, installiert der Management-Blade-Server das Scan-Software-Image automatisch auf dem neuen Blade. Welches Scan-Software-Image installiert wird, hängt davon ab, welche Optionen Sie bei der Konfiguration Ihres Blade-Servers auswählen.

Sie können entweder die in der Software des Content Security Blade Server enthaltenen Web-Scan-Funktionen oder auf einigen oder allen Blade-Servern zum Scannen von Inhalten die Software McAfee Web Gateway 6.8.7 (vormals WebWasher) installieren. Sie können Folgendes installieren:

- Email and Web Security-Software – Mit dieser Option wird die Software auf allen Blade-Servern zum Scannen von Inhalten installiert, und jedes Blade scannt sowohl E-Mails als auch Web-Verkehr.
- Email Security-Software – Sie können auswählen, auf welchen Blade-Servern zum Scannen von Inhalten die Email Security-Software installiert werden soll.
- Web Security-Software – Sie können auswählen, auf welchen Blade-Servern zum Scannen von Inhalten die Web Security-Software installiert werden soll.
- McAfee Web Gateway-Software – Sie können auswählen, auf welchen Blade-Servern zum Scannen von Inhalten die McAfee Web Gateway-Software (vormals WebWasher) installiert werden soll.

HINWEIS: Wenn Sie McAfee Web Gateway-Software auswählen und installieren, können Sie auf demselben Chassis nur entweder die Email and Web Security-Software oder die Web Security-Software installieren. Sie müssen außerdem Ihren Blade-Server im Modus "Expliziter Proxy" installieren, wenn Sie McAfee Web Gateway-Software verwenden möchten.

Jeder Blade-Server zum Scannen von Inhalten beginnt unmittelbar nach der Installation der Software mit dem Scannen.

Ein Blade-Server zum Scannen von Inhalten wird nur zum Scannen Ihres Datenverkehrs verwendet. Er ist kein Management-Blade-Server. Der Blade-Server zum Scannen von Inhalten:

- Empfängt die DAT-Dateien und Software-Patches vom Management-Blade-Server.
- Sendet Informationen zu allen Scan- und Erkennungsereignissen an den Management-Blade-Server.
- Sendet Informationen zu allen isolierten und zurückgestellten E-Mails und Dateien an den Management-Blade-Server.

Vorbereitung der Installation

Um den sicheren Betrieb des Produkts zu gewährleisten, beachten Sie Folgendes, bevor Sie mit der Installation beginnen.

- Lernen Sie die stromtechnischen Anforderungen Ihres Blade-Servers und Ihres Stromversorgungssystems kennen.
- Machen Sie sich mit den Betriebsmodi und den Funktionen vertraut. Es ist wichtig, dass Sie eine gültige Konfiguration auswählen.
- Entscheiden Sie, wie Sie den Blade-Server in Ihr Netzwerk integrieren möchten, und stellen Sie fest, welche Informationen Sie benötigen, bevor Sie beginnen. Sie benötigen beispielsweise den Namen und die IP-Adresse des Blade-Servers.
- Packen Sie das Produkt so nah wie möglich am vorgesehenen Aufstellungsort aus.
- Nehmen Sie das Produkt aus der Schutzverpackung, und stellen Sie es auf eine ebene Fläche.
- Beachten Sie alle Sicherheitswarnungen.

VORSICHT: Lesen Sie alle mitgelieferten Sicherheitsinformationen, und machen Sie sich mit ihnen vertraut.

Inhalt

▸ Platzieren des Blade-Servers

Lieferumfang

Überprüfen Sie anhand der mit dem Produkt ausgelieferten Packliste, ob alle Komponenten enthalten sind.

Folgendes sollte vorhanden sein:

- Ein Blade-Server-Gehäuse (entweder ein M3- oder ein M7-Gehäuse)
- Ein Management-Blade-Server
- Ein Failover-Management-Blade-Server
- Ein oder mehrere Scan-Blades, abhängig von der Bestellung
- Netzkabel
- Netzwerkkabel
- Installations- und Wiederherstellungs-CD für Email and Web Security
- CD mit dem Linux-Quellcode
- CD mit McAfee Quarantine Manager
- Dokumentations-CD

Wenn ein Element fehlt oder beschädigt ist, setzen Sie sich mit dem Händler in Verbindung.

Planen der Installation

Bevor Sie den Content Security Blade Server auspacken, sollten Sie unbedingt die Installation und Ausbringung planen.

Informationen hierzu finden Sie im: HP BladeSystem c-Class Site Planning Guide.

Beachten Sie Folgendes:

- Allgemeine Richtlinien zum Vorbereiten Ihres Standorts

  Übersichten über die allgemeinen Anforderungen an den Standort zur Vorbereitung Ihres Computer-Raums für die Content Security Blade Server-Hardware.

- Umgebungsanforderungen

  Informationen zu den Umgebungsanforderungen, einschließlich Temperatur, Belüftung und Platzbedarf.

- Stromanforderungen und Überlegungen

  Stromanforderungen und elektrische Faktoren, die vor der Installation bedacht werden müssen.

  Umfasst die Installation der Power Distribution Unit (PDU).

- Hardware-Spezifikationen und -Anforderungen

  Systemspezifikationen für das Blade-Server-Gehäuse, Racks und einphasige und dreiphasige Stromquellen.

- Konfigurationsszenarien
- Vorbereitung der Installation

Unangemessene Nutzung

Das Produkt ist:

- **Keine Firewall.** Es muss in Ihrer Organisation hinter einer ordnungsgemäß konfigurierten Firewall verwendet werden.
- **Kein Server zum Speichern zusätzlicher Software und Dateien.** Installieren Sie keine Software auf dem Gerät, und fügen Sie keine zusätzlichen Dateien hinzu, es sei denn, Sie werden in der Produktdokumentation oder von Ihrem Support-Mitarbeiter dazu aufgefordert. Das Gerät kann nicht alle Arten von Datenverkehr verarbeiten. Wenn Sie den Modus "Expliziter Proxy" verwenden, sollten nur Protokolle an das Gerät gesendet werden, die gescannt werden müssen.

Platzieren des Blade-Servers

Installieren Sie den Blade-Server so, dass Sie den physischen Zugang zur Einheit steuern und auf die Anschlüsse und Verbindungen zugreifen können.

Mit dem Chassis des Blade-Servers wird ein Set zur Montage in einem Rack ausgeliefert, mit dem Sie den Blade-Server in einem 19-Zoll-Rack installieren können.

Siehe HP BladeSystem c3000 Enclosure Quick Setup Instructions oder HP BladeSystem c7000 Enclosure Quick Setup Instructions.

Überlegungen zu Netzwerkmodi

Bevor Sie Ihren Content Security Blade Server installieren und konfigurieren, müssen Sie sich überlegen, welchen Netzwerkmodus Sie verwenden möchten. Vom ausgewählten Modus hängt es ab, wie Sie Ihren Blade-Server physisch an Ihr Netzwerk anschließen.

Sie können einen der folgenden Netzwerkmodi auswählen.

- **Modus "Transparente Bridge"** – Das Gerät fungiert als Ethernet-Bridge.
- **Modus "Transparenter Router"** – Das Gerät fungiert als Router.
- **Modus "Expliziter Proxy"** – Das Gerät fungiert als Proxy-Server und Mail-Relay.

Wenn Sie nach der Lektüre dieses und der folgenden Abschnitte weiterhin unsicher sind, welchen Modus Sie verwenden sollen, sprechen Sie mit einem Netzwerkexperten.

VORSICHT: Falls Sie vorhaben, auf einem oder mehreren Scan-Blades die Software "McAfee Web Gateway" (vormals WebWasher) auszuführen, müssen Sie Ihren Blade-Server im Modus "Expliziter Proxy" konfigurieren.

Architektonische Aspekte hinsichtlich der Netzwerkmodi

Hinsichtlich der Netzwerkmodi müssen Sie vor allem folgende Aspekte bedenken:

- Ob Kommunikationsgeräte die Existenz des Geräts kennen. Das heißt, ob das Gerät in einem der transparenten Modi arbeitet.
- Wie das Gerät physisch mit Ihrem Netzwerk verbunden wird.
- Die erforderliche Konfiguration zur Integration des Geräts in Ihr Netzwerk.
- An welchem Ort im Netzwerk die Konfiguration erfolgt.

Überlegungen vor dem Ändern des Netzwerkmodus

In den Modi "Expliziter Proxy" und "Transparenter Router" können Sie das Gerät so einrichten, dass es sich innerhalb mehrerer Netzwerke befindet. Dies wird durch das Einrichten mehrerer IP-Adressen für die LAN1- und LAN2-Anschlüsse ermöglicht.

Wenn Sie aus dem Modus "Expliziter Proxy" oder "Transparenter Router" in den Modus "Transparente Bridge" wechseln, wird nur die aktivierte IP-Adresse für jeden Anschluss übernommen.

TIPP: Nachdem ein Netzwerkmodus festgelegt wurde, empfiehlt es sich, diesen nicht mehr zu ändern, es sei denn, der Standort des Geräts ändert sich oder das Netzwerk wird neu strukturiert.

Inhalt

▸ Modus "Transparente Bridge"
▸ Modus "Expliziter Proxy"

Modus "Transparente Bridge"

Im Modus "Transparente Bridge" bemerken die kommunizierenden Server das Gerät nicht. Der Betrieb des Geräts ist für die Server transparent.

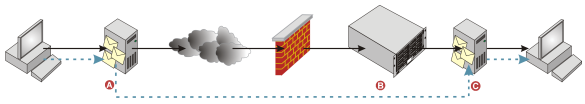


Abbildung 1: Transparente Kommunikation

In Abbildung 1: Transparente Kommunikation sendet der externe E-Mail-Server (**A**) E-Mails an den internen E-Mail-Server (**C**). Der externe Mail-Server kann nicht erkennen, dass die von ihm gesendete E-Mail-Nachricht vom Gerät abgefangen und gescannt wird (**B**).

Der externe E-Mail-Server scheint direkt mit dem internen E-Mail-Server zu kommunizieren (der Pfad wird als gestrichelte Linie dargestellt). Tatsächlich wird der Datenverkehr möglicherweise durch mehrere Netzwerkgeräte geleitet und vom Gerät abgefangen und gescannt, bevor er den internen Mail-Server erreicht.

Funktion des Geräts

Im Modus "Transparente Bridge" wird das Gerät über den LAN1- und den LAN2-Anschluss mit dem Netzwerk verbunden. Das Gerät scannt den empfangenen Datenverkehr und fungiert als Bridge, die zwei Netzwerksegmente verbindet, behandelt diese aber wie ein einziges logisches Netzwerk.

Konfiguration

Der Modus "Transparente Bridge" erfordert weniger Konfigurationsaufwand als die Modi "Transparenter Router" oder "Expliziter Proxy". Sie müssen nicht alle Clients, das Standard-Gateway, MX-Einträge, Firewall-NAT und E-Mail-Server neu konfigurieren, damit der Datenverkehr an das Gerät gesendet wird. Da das Gerät in diesem Modus nicht als Router fungiert, ist es auch nicht erforderlich, eine Routing-Tabelle zu aktualisieren.

Platzieren des Geräts

Aus Sicherheitsgründen sollten Sie das Gerät innerhalb Ihres Unternehmens und hinter einer Firewall betreiben.

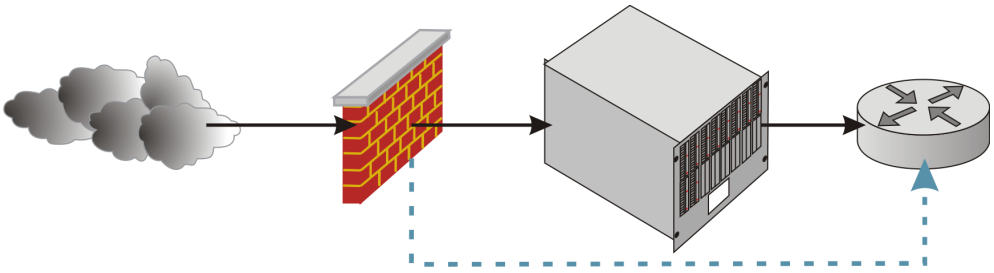


Abbildung 2: Einzelnes logisches Netzwerk

TIPP: Im Modus "Transparente Bridge" positionieren Sie das Gerät zwischen der Firewall und Ihrem Router, wie in Abbildung 2: Einzelnes logisches Netzwerk dargestellt.

In diesem Modus verbinden Sie zwei Netzwerksegmente physisch mit dem Gerät. Das Gerät behandelt diese als eine einzige logische Einheit. Da sich die Geräte – Firewall, Gerät und Router – im selben logischen Netzwerk befinden, müssen sie kompatible IP-Adressen im selben Subnetz haben.

Geräte auf der einen Seite der Bridge (z. B. ein Router), die mit den Geräten auf der anderen Seite der Bridge (z. B. einer Firewall) kommunizieren, bemerken die Bridge nicht. Sie erkennen

nicht, dass der Datenverkehr abgefangen und gescannt wird. Deshalb wird dieser Betriebsmodus des Geräts als "Transparente Bridge" bezeichnet.

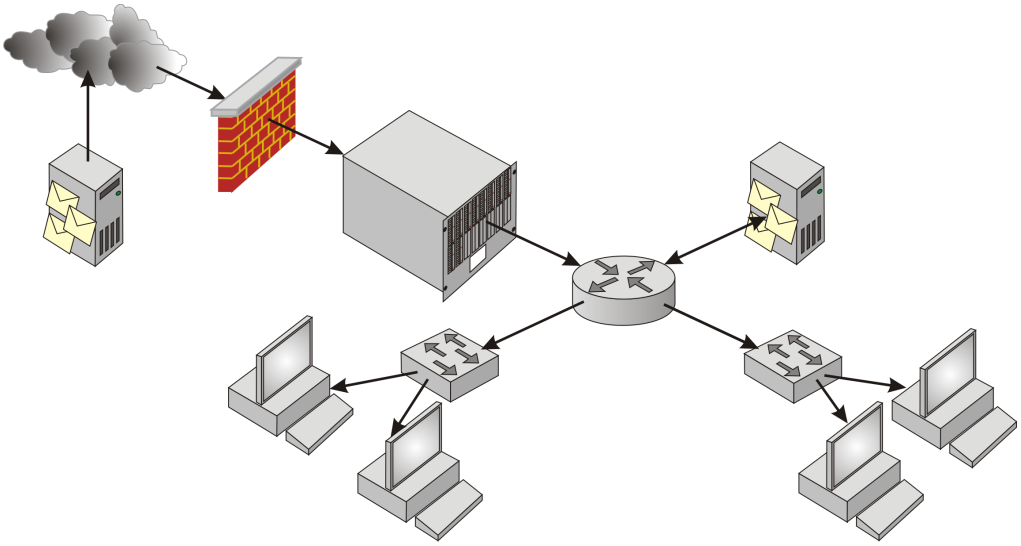


Abbildung 3: Modus "Transparente Bridge"

Das Spanning Tree-Protokoll zum Verwalten der Bridge-Priorität

Sollte ein Blade ausfallen, leitet das Spanning Tree-Protokoll (STP) den Netzwerkverkehr an das Blade mit der nächsthöheren Bridge-Priorität weiter.

Im Modus "Transparente Bridge" haben der Management-Blade-Server und der Failover-Management-Blade-Server unterschiedliche IP-Adressen.

In den Modi "Transparenter Router" und "Expliziter Proxy" haben die beiden Blades ebenfalls unterschiedliche IP-Adressen, werden jedoch mit derselben virtuellen IP-Adresse bzw. mit denselben virtuellen IP-Adressen konfiguriert.

Normalerweise wird der E-Mail-Verkehr vom Management-Blade-Server verarbeitet. Falls dieses Blade ausfällt, wird der E-Mail-Verkehr vom Failover-Management-Blade-Server verarbeitet.

Jedes Blade hat eine andere Bridge-Priorität. Da der Management-Blade-Server über eine höhere Priorität verfügt (beispielsweise den STP-Wert 100), scannt normalerweise der Management-Blade-Server den Netzwerkverkehr. Sollte der Management-Blade-Server ausfallen, leitet das STP den Netzwerkverkehr über einen Pfad mit der nächsthöheren Bridge-Priorität weiter, also an den Failover-Management-Blade-Server (beispielsweise mit einem STP-Wert von 200).

So konfigurieren Sie den Blade-Server:

1. Gehen Sie folgendermaßen vor, um Bridge-Loops zu vermeiden:
   - **a** Deaktivieren Sie STP auf den Anschlüssen 1 und 2 aller Interconnect-Module.
   - **b** Stellen Sie sicher, dass alle Anschlüsse Mitglieder von STG1 sind.
   - **c** Deaktivieren Sie STG1.
2. Installieren Sie den Failover-Management-Blade-Server in Steckplatz 2.
3. Während der Einrichtung des Failover-Management-Blade-Servers stellen Sie für die Bridge-Priorität beispielsweise den Wert "200" ein.
4. Installieren Sie den Management-Blade-Server in Steckplatz 1.

5 Während der Einrichtung des Management-Blade-Servers stellen Sie für die Bridge-Priorität beispielsweise den Wert "100" ein.

6 Geben Sie dem Management-Blade-Server und dem Failover-Management-Blade-Server unterschiedliche IP-Adressen.

Modus "Transparenter Router"

Im Modus "Transparenter Router" scannt das Gerät den E-Mail-Verkehr zwischen zwei Netzwerken. Jede Schnittstelle hat eine oder mehrere IP-Adressen.

Die kommunizierenden Netzwerkserver erkennen nicht, dass das Gerät zwischengeschaltet ist. Der Betrieb des Geräts ist für die Geräte *transparent*.

- Funktion des Geräts
- Konfiguration
- Firewall-Regeln
- Platzieren des Geräts

Funktion des Geräts

Im Modus "Transparenter Router" wird das Gerät mit den Netzwerken über den LAN1- und den LAN2-Anschluss verbunden. Das Gerät scannt den Datenverkehr, der über ein Netzwerk eingeht, und leitet ihn an das nächste Netzwerkgerät in einem anderen Netzwerk weiter. Das Gerät fungiert als Router (wobei es Datenverkehr zwischen den verschiedenen Netzwerken auf der Basis der Informationen in den Routing-Tabellen weiterleitet).

Konfiguration

Im Modus "Transparenter Router" müssen Sie Ihre Netzwerkgeräte nicht explizit neu konfigurieren, damit der Datenverkehr an das Gerät gesendet wird. Sie müssen lediglich die Routing-Tabelle für das Gerät konfigurieren und einige der Routing-Informationen für die Netzwerkgeräte auf einer Seite des Geräts ändern (der Geräte also, die an die LAN1- und LAN2-Anschlüsse des Geräts angeschlossen sind). Es könnte zum Beispiel erforderlich sein, das Gerät als Standard-Gateway zu konfigurieren.

Im Modus "Transparenter Router" muss das Gerät zwei Netzwerke miteinander verbinden. Das Gerät muss innerhalb Ihres Unternehmens hinter einer Firewall positioniert werden.

HINWEIS: Im Modus "Transparenter Router" werden weder Multicast-IP-Datenverkehr noch andere Protokolle wie NETBEUI und IPX (Nicht-IP-Protokolle) unterstützt.

Firewall-Regeln

Im Modus "Transparenter Router" wird die Firewall mit der physischen IP-Adresse für die LAN1/LAN2-Verbindung mit dem Management-Blade-Server verbunden.

Platzieren des Geräts

Verwenden Sie das Gerät im Modus "Transparenter Router", um einen im Netzwerk vorhandenen Router zu ersetzen.

TIPP: Wenn Sie den Modus "Transparenter Router" verwenden und keinen vorhandenen Router ersetzen, müssen Sie einen Teil Ihres Netzwerks neu konfigurieren, damit der Datenverkehr korrekt durch das Gerät fließt.

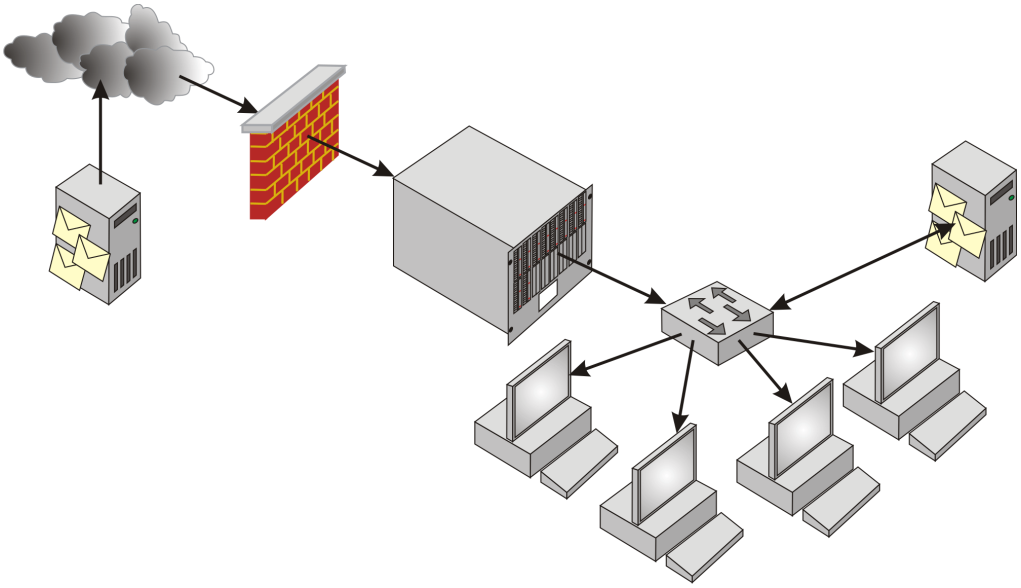


Abbildung 4: Konfiguration im Modus "Transparenter Router"

Sie müssen wie folgt vorgehen:

- Konfigurieren Sie die Client-Geräte so, dass sie auf das Standard-Gateway verweisen.
- Konfigurieren Sie das Gerät so, dass das Internet-Gateway als Standard-Gateway verwendet wird.
- Stellen Sie sicher, dass Ihre Client-Geräte E-Mails an die E-Mail-Server in Ihrem Unternehmen senden können.

Modus "Expliziter Proxy"

Im Modus "Expliziter Proxy" müssen einige Netzwerkgeräte so eingerichtet werden, dass sie Datenverkehr explizit an das Gerät senden. Das Gerät fungiert dann als Proxy oder Relay und verarbeitet den Datenverkehr für die Geräte.

Der Modus "Expliziter Proxy" ist am besten für Netzwerke geeignet, in denen Client-Geräte über ein einzelnes Upstream- und Downstream-Gerät eine Verbindung zum Gerät herstellen.

TIPP: Dies ist möglicherweise nicht die beste Option, wenn verschiedene Netzwerkgeräte erneut konfiguriert werden müssen, damit sie den Datenverkehr an das Gerät senden.

Netzwerk- und Gerätekonfiguration

Wenn sich das Gerät im Modus "Expliziter Proxy" befindet, müssen Sie den internen Mail-Server explizit so konfigurieren, dass er E-Mail-Verkehr an das Gerät sendet. Das Gerät prüft den E-Mail-Verkehr, bevor es ihn im Namen des Absenders an den externen Mail-Server weiterleitet. Der externe E-Mail-Server leitet die E-Mail dann an den Empfänger weiter.

Entsprechend muss das Netzwerk so konfiguriert werden, dass eingehende E-Mail-Nachrichten aus dem Internet nicht dem internen Mail-Server, sondern dem Gerät zugestellt werden.

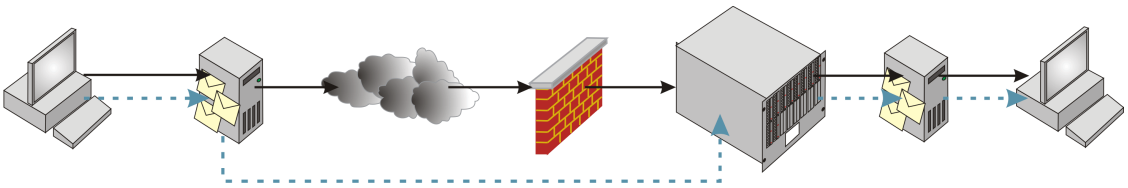


Abbildung 5: Weiterleiten des E-Mail-Verkehrs

Das Gerät kann den E-Mail-Verkehr dann prüfen, bevor es ihn im Namen des Absenders an den internen Mail-Server zur Zustellung weiterleitet, wie in Abbildung 5: Weiterleiten des E-Mail-Verkehrs dargestellt.

Beispielsweise kann ein externer Mail-Server direkt mit dem Gerät kommunizieren, auch wenn der Datenverkehr möglicherweise mehrere Netzwerkserver passiert, bevor er das Gerät erreicht. Der wahrgenommene Pfad verläuft vom externen Mail-Server zum Gerät.

Protokolle

Um ein unterstütztes Protokoll zu scannen, müssen Sie Ihre anderen Netzwerkserver oder Client-Computer so konfigurieren, dass das Protokoll durch das Gerät geleitet wird, sodass kein Datenverkehr das Gerät umgehen kann.

Firewall-Regeln

Im Modus "Expliziter Proxy" werden alle Firewall-Regeln, die für den Client-Zugriff auf das Internet eingerichtet wurden, außer Kraft gesetzt. Für die Firewall sind nur die IP-Adressinformationen für das Gerät sichtbar, nicht die IP-Adressen der Clients. Dies bedeutet, dass die Firewall ihre Internetzugriffsregeln nicht auf die Clients anwenden kann.

Platzieren des Geräts

Konfigurieren Sie die Netzwerkgeräte so, dass der zu scannende Datenverkehr an das Gerät gesendet wird. Das ist wichtiger als der Standort des Geräts.

Der Router muss allen Benutzern erlauben, eine Verbindung zum Gerät herzustellen.

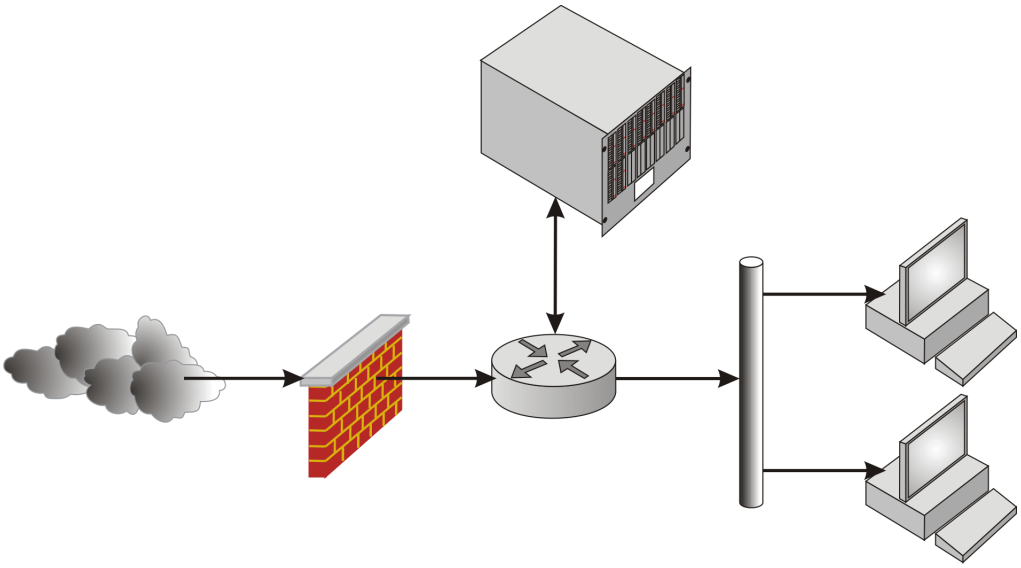


Abbildung 6: Konfiguration als expliziter Proxy

Das Gerät muss innerhalb Ihres Unternehmens hinter einer Firewall positioniert werden, wie in Abbildung 6: Konfiguration als expliziter Proxy dargestellt.

Normalerweise ist die Firewall so konfiguriert, dass der Datenverkehr, der nicht direkt von dem Gerät stammt, gesperrt wird.

Wenn Sie in Bezug auf die Topologie Ihres Netzwerks unsicher sind und nicht wissen, wie Sie das Gerät integrieren sollen, wenden Sie sich an Ihren Netzwerkspezialisten.

Verwenden Sie diese Konfiguration in folgenden Fällen:

- Das Gerät wird im Modus "Expliziter Proxy" betrieben.
- Sie verwenden E-Mail (SMTP).

Für diese Konfiguration gilt:

- Konfigurieren Sie die externen DNS-Server (Domain Name System) oder NAT (Network Address Translation) auf der Firewall so, dass der externe Mail-Server E-Mails an das Gerät zustellt, nicht an den internen Mail-Server.
- Konfigurieren Sie die internen Mail-Server so, dass E-Mail-Verkehr an das Gerät gesendet wird. Das heißt, die internen Mail-Server müssen das Gerät als Smart-Host verwenden. Vergewissern Sie sich, dass die Client-Geräte E-Mails an die E-Mail-Server in Ihrem Unternehmen senden können.
- Stellen Sie sicher, dass die Firewall-Regeln aktualisiert werden. Die Firewall muss den Datenverkehr von dem Gerät akzeptieren, darf aber keinen Datenverkehr verarbeiten, der direkt von den Client-Geräten kommt. Richten Sie Regeln ein, die verhindern, dass unerwünschter Datenverkehr in Ihr Unternehmen gelangt.

Ausbringungsstrategien für die Verwendung des Geräts in einer DMZ

Eine "demilitarisierte Zone" (Demilitarized Zone, DMZ) ist ein Netzwerk, das durch eine Firewall von allen anderen Netzwerken getrennt ist, auch vom Internet und anderen internen Netzwerken.

Eine DMZ wird üblicherweise mit dem Ziel implementiert, den Zugriff auf Server zu sperren, die Internetdienste (beispielsweise E-Mail) zur Verfügung stellen.

Hacker verschaffen sich oft Zugriff auf Netzwerke, indem sie herausfinden, auf welchen TCP-/UDP-Ports Appliances Anfragen erwarten, und dann bekannte Schwachstellen in Appliances ausnutzen. Firewalls senken das Risiko solcher Exploits erheblich, indem sie den Zugriff auf bestimmte Ports auf bestimmten Servern steuern.

Das Gerät kann einfach zu einer DMZ-Konfiguration hinzugefügt werden. Die Art, wie Sie das Gerät in einer DMZ verwenden, hängt von den zu scannenden Protokollen ab.

Inhalt

- SMTP-Konfiguration in einer DMZ
- Arbeitslastverwaltung
- Integrierte Redundanz

SMTP-Konfiguration in einer DMZ

Die DMZ ist eine gute Möglichkeit für das Verschlüsseln von E-Mails. Wenn der E-Mail-Verkehr die Firewall zum zweiten Mal erreicht (auf seinem Weg von der DMZ zum internen Netzwerk), ist er verschlüsselt.

Geräte, die SMTP-Verkehr in einer DMZ scannen können, sind normalerweise im Modus "Expliziter Proxy" konfiguriert.

Konfigurationsänderungen müssen nur an den MX-Einträgen für die E-Mail-Server vorgenommen werden.

HINWEIS: Sie können den Modus "Transparente Bridge" verwenden, wenn Sie SMTP in einer DMZ scannen. Wenn Sie jedoch den Datenfluss nicht richtig steuern, scannt das Gerät jede Nachricht zweimal, einmal in jede Richtung. Aus diesem Grund wird für SMTP-Scans normalerweise der Modus "Expliziter Proxy" verwendet.

E-Mail-Relay

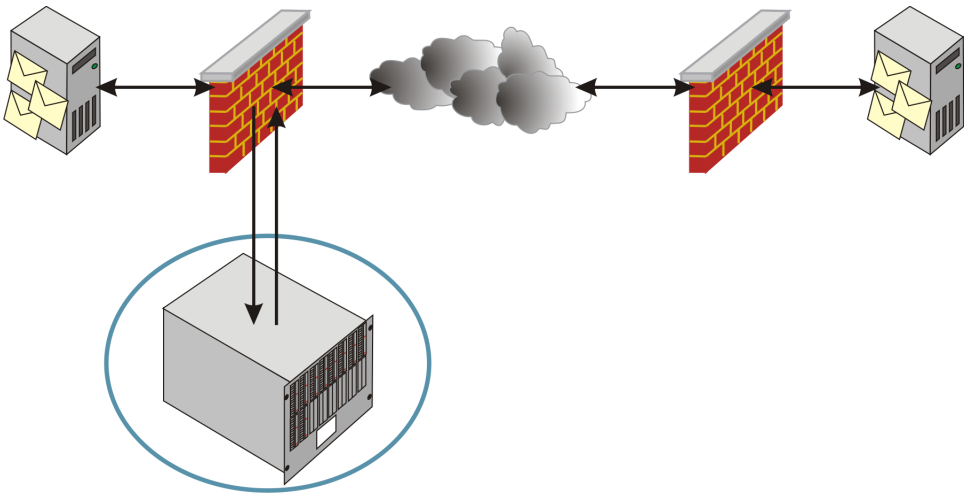


Abbildung 7: Konfiguration eines Geräts im Modus "Expliziter Proxy" in einer DMZ

Wenn Sie in Ihrer DMZ bereits ein Relay eingerichtet haben, können Sie es durch das Gerät ersetzen.

Um Ihre bestehenden Firewall-Richtlinien zu verwenden, geben Sie dem Gerät dieselbe IP-Adresse wie dem Mail-Relay.

E-Mail-Gateway

SMTP bietet keine Methoden zur Verschlüsselung von E-Mail-Nachrichten. Sie können mithilfe von TLS (Transport Layer Security) den Link verschlüsseln, nicht jedoch die E-Mail-Nachrichten. Daher erlauben einige Unternehmen solchen Datenverkehr nicht in ihrem internen Netzwerk. Zur Umgehung dieses Problems wird häufig ein proprietäres E-Mail-Gateway eingesetzt, zum Beispiel Lotus Notes® oder Microsoft® Exchange, um den E-Mail-Datenverkehr zu verschlüsseln, bevor er das interne Netzwerk erreicht.

Um eine DMZ-Konfiguration unter Verwendung des proprietären E-Mail-Gateways zu implementieren, fügen Sie das Scan-Gerät zur DMZ auf der SMTP-Seite des Gateways hinzu.

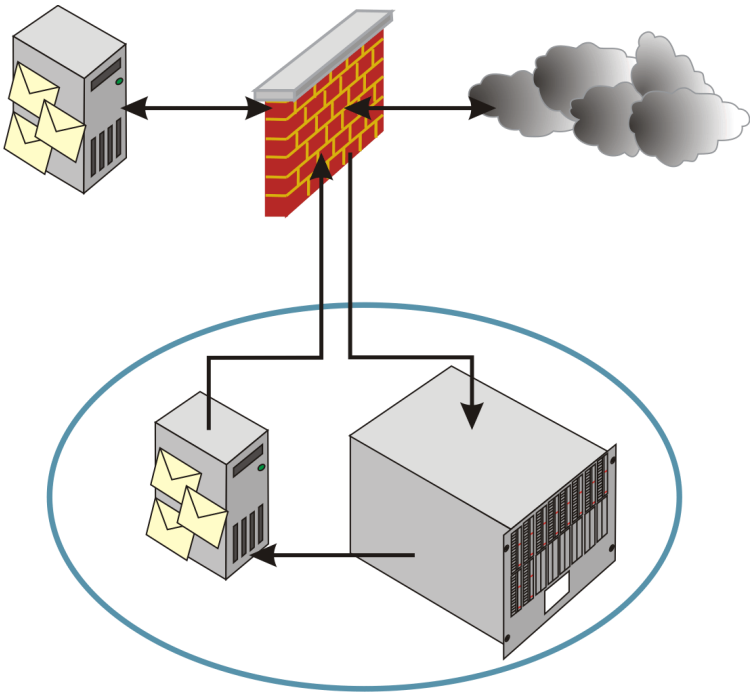


Abbildung 8: Schützen eines E-Mail-Gateways in einer DMZ

Nehmen Sie hierfür folgende Konfigurationen vor:

- Die öffentlichen MX-Einträge müssen externe Mail-Server anweisen, alle eingehenden E-Mail-Nachrichten an das Gerät (statt an das Gateway) zu senden.
- Das Gerät muss alle eingehenden E-Mail-Nachrichten an das Mail-Gateway und alle ausgehenden Nachrichten per DNS oder über ein externes Relay senden.
- Das E-Mail-Gateway muss alle eingehenden E-Mails an die internen Mail-Server und aller andere (ausgehenden) Mails an das Gerät weiterleiten.
- Die Firewall erlaubt nur eingehende E-Mails, die sich an das Gerät richten.

HINWEIS: Bei Firewalls, auf denen die Verwendung von NAT (Network Address Translation) konfiguriert ist und die eingehende E-Mails an die internen E-Mail-Server umleiten, müssen die öffentlichen MX-Einträge nicht neu konfiguriert werden. Sie leiten den Datenverkehr bereits an die Firewall und nicht an das eigentliche E-Mail-Gateway. In diesem Fall muss die Firewall neu konfiguriert werden, sodass eingehende Nachrichten an das Gerät geleitet werden.

Für Lotus Notes spezifische Firewall-Regeln

Lotus Notes-Server kommunizieren standardmäßig über TCP-Port 1352. Die für den Schutz von Notes-Servern in einer DMZ verwendeten Firewall-Regeln erlauben üblicherweise folgendem Datenverkehr das Passieren durch die Firewall:

- Eingehende SMTP-Anforderungen (TCP-Port 25) vom Internet, die für das Gerät bestimmt sind
- Anforderungen auf TCP-Port 1352 aus dem Notes-Gateway, die an einen internen Notes-Server gerichtet sind
- Anforderungen auf TCP-Port 1352 von einem internen Notes-Server, die an das Notes-Gateway gerichtet sind
- SMTP-Anforderungen vom Gerät, die für das Internet bestimmt sind

Alle anderen SMTP-Anforderungen und Anforderungen auf TCP-Port 1352 werden verweigert.

Für Microsoft Exchange spezifische Firewall-Regeln

Ein auf Microsoft Exchange basierendes E-Mail-System erfordert eine erhebliche Umkonfiguration.

Wenn Exchange-Server miteinander kommunizieren, senden sie die ersten Pakete mithilfe des RPC-Protokolls (TCP-Port 135). Sobald die ursprüngliche Kommunikation jedoch eingerichtet ist, werden zwei Ports dynamisch ausgewählt und verwendet, um alle nachfolgenden Pakete für den Rest der Kommunikation zu senden. Sie können die Firewall nicht so konfigurieren, dass sie diese dynamisch gewählten Ports erkennt. Deshalb leitet die Firewall diese Pakete nicht weiter.

Die Ausweichlösung lautet, die Registrierung auf jedem Exchange-Server zu modifizieren, der über die Firewall kommuniziert, sodass immer dieselben zwei "dynamischen" Ports verwendet werden, und dann TCP 135 und diese beiden Ports auf der Firewall zu öffnen.

Wir erwähnen diese Ausweichlösung, um eine umfassende Erklärung zu bieten, wir empfehlen sie jedoch nicht. Das RPC-Protokoll ist in Microsoft-Netzwerken weit verbreitet. Das Öffnen von TCP 135 für eingehenden Datenverkehr ist für die meisten Sicherheitsexperten ein rotes Tuch.

Wenn Sie diese Ausweichlösung verwenden möchten, finden Sie Details in den folgenden KnowledgeBase-Artikeln auf der Microsoft-Website:

- Q155831
- Q176466

Arbeitslastverwaltung

Der Blade-Server verfügt über eine eigene interne Arbeitslastverwaltung, durch die die Scan-Last gleichmäßig auf alle im Gehäuse installierten Scan-Blades verteilt wird.

Sie müssen keinen separaten externen Lastenausgleicher bereitstellen.

Integrierte Redundanz

Beim McAfee® Content Security Blade Server wird, wenn ein Blade-Server zum Scannen von Inhalten ausfällt, die Arbeit durch die Arbeitslastverwaltungsfunktionen zwischen den übrigen Blade-Servern zum Scannen von Inhalten verteilt.

Wenn der Management-Blade-Server ausfällt, übernimmt der Failover-Management-Blade-Server die weitere Arbeitslastverwaltung, wodurch ein ausgesprochen zuverlässiges Scannen gewährleistet wird.

Der Blade-Server verfügt über eine Redundanz innerhalb des Gehäuses, da mehrere Stromversorgungen und Kühllüfter vorhanden sind. Wenn eine Stromversorgung oder ein Lüfter ausfällt, bleibt der Blade-Server in Betrieb, und die fehlerhafte Komponente kann ausgetauscht werden, ohne dass der Blade-Server heruntergefahren werden muss.

Wenn Sie den Blade-Server für den ausfallsicheren Modus konfigurieren, können Sie zusätzlich die Immunität des Blade-Servers vor einem Ausfall der Netzwerkverbindung verbessern. Dies betrifft sowohl Ausfälle der Verbindungen innerhalb des Gehäuses oder zu einem externen Netzwerk, beispielsweise durch ein beschädigtes Kabel oder die Trennung der Verbindung. Siehe Betrieb im ausfallsicheren Modus.

Planen der Installation

Häufig bestimmt die Konfiguration des bestehenden Netzwerks die Art und Weise, wie der Blade-Server in das Netzwerk integriert werden sollte.

Bevor Sie den Blade-Server ausbringen, sollten Sie die Diagramme Ihrer Netzwerktopografie analysieren und sich mit Ihrem vorhandenen Netzwerk vertraut machen.

Sie nutzen den neuen Blade-Server am besten, wenn Sie den Datenverkehr in Ihrem bestehenden Netzwerk sorgfältig überwachen und analysieren, welchen Einfluss die Integration des Blade-Servers darauf nehmen wird.

Inhalt

- Vor dem Start einer Standardinstallation
- Vor dem Installieren des Gehäuses
- Einrichten der Lights-Out-Verwaltung
- Nach der Installation

Vor dem Start einer Standardinstallation

McAfee empfiehlt, dass Sie vor der Konfiguration Ihres McAfee® Content Security Blade Servers Folgendes ermitteln:

- IP-Adressen

  Jedes Content Security Blade Server-Gehäuse benötigt IP-Adressen für folgende Komponenten:

  - Onboard-Administrator-Modul (OA)
  - Integrierte Lights-Out-Module (iLO) (zwischen 8 und 16 Adressen, abhängig von der Konfiguration)
  - Interconnect-Module (x2)
  - IP-Adresse für Out-of-Band-Verwaltung (OOB) des Management-Blade-Servers
  - LAN-IP-Adresse des Management-Blade-Servers (1 oder 2, abhängig vom Betriebsmodus)
  - OOB-IP-Adresse des Failover-Management-Blade-Servers
  - LAN-IP-Adresse des Failover-Management-Blade-Servers (1 oder 2, abhängig vom Betriebsmodus)
  - Virtuelle IP-Adresse des Systems (1 oder 2, abhängig vom Betriebsmodus)
- Firmware-Versionen

Die Hardware muss durch Upgrades auf mindestens folgenden Stand gebracht werden:

- Onboard Administrator – v3.21
- HP GbE2c Interconnect-Module – v5.1.3
- Blade BIOS (G6-Blades) – I24 03/30/2010
- Blade BIOS (G1-Blades) – I15 07/10/2009
- Blade iLO – 1.82

HINWEIS: Sie können das ISO-Image *Smart Update Firmware DVD ISO, v9.10 (C) - August 30, 2010* mit den Firmware-Versionen von http://www.hp.com/go/bladesystemupdates/ herunterladen.

- Netzwerkdiagramm

  Es ist hilfreich, über Netzwerkdiagramme zu verfügen, die zeigen, wie die gehäuseinternen Netzwerke des Content Security Blade Servers (LAN1, LAN2, OOB und OA) in Ihre vorhandene Netzwerkinfrastruktur integriert werden.

  Für Installationen im Modus "Transparente Bridge" ist es wichtig zu wissen, welche der VLANs über Bridges verbunden werden.

Vor dem Installieren des Gehäuses

Bestimmen Sie vor der Installation des Gehäuses Folgendes:

- Strom und Belüftung
- Netzwerkmodus
- Netzwerkadressen
- Onboard Administrator
- Lights-Out-Verwaltung
- Failover-Anforderungen

Strom und Belüftung

Um die Anforderungen bezüglich Strom und Belüftung für das Gehäuse mit der erwarteten Anzahl an Blades zu bestimmen, siehe:

- *HP BladeSystem cClass Solution Overview*
- Für M3-Gehäuse: *HP BladeSystem c3000 Enclosure Setup and Installation Guide*
- Für M7-Gehäuse: *HP BladeSystem c7000 Enclosure Setup and Installation Guide*
- *HP BladeSystem Power Sizer Tool*

Netzwerkmodus

Sie müssen bestimmen, welcher Netzwerkmodus für die Installation verwendet werden soll:

- Modus "Transparenter Router"
- Modus "Transparente Bridge"
- Modus "Expliziter Proxy"

IP-Adressen

Jedes Content Security Blade Server-Gehäuse benötigt IP-Adressen für folgende Komponenten:

- Onboard-Administrator-Modul (OA)
- Integrierte Lights-Out-Module (iLO) (zwischen 8 und 16 Adressen, abhängig von der Konfiguration)
- Interconnect-Module (x2)
- IP-Adresse für Out-of-Band-Verwaltung (OOB) des Management-Blade-Servers
- LAN-IP-Adresse des Management-Blade-Servers (1 oder 2, abhängig vom Betriebsmodus)
- OOB-IP-Adresse des Failover-Management-Blade-Servers
- LAN-IP-Adresse des Failover-Management-Blade-Servers (1 oder 2, abhängig vom Betriebsmodus)
- Virtuelle IP-Adresse des Systems (1 oder 2, abhängig vom Betriebsmodus)

Onboard Administrator

Wenn Sie den Onboard Administrator einrichten, gehen Sie wie folgt vor:

- Konfigurieren Sie den Onboard Administrator über die Chassis-Anzeige.
- Melden Sie sich über HTTP bei der Benutzeroberfläche des Onboard Administrator an.
- Führen Sie den Setup-Assistenten des Onboard Administrator aus.

Für M3-Gehäuse, siehe: HP BladeSystem c3000 Enclosure Setup and Installation Guide

Für M7-Gehäuse, siehe: HP BladeSystem c7000 Enclosure Setup and Installation Guide.

Lights-Out-Verwaltung

Sie müssen für die Lights-Out-Verwaltung Ihre Netzwerkinfrastruktur ermitteln.

Failover-Anforderungen

Die Failover-Anforderungen hängen von dem für die Konfiguration des Blade-Servers verwendeten Modus ab.

- Modus "Transparente Bridge"

  Die Bridge-Priorität (STP-Einstellung) bestimmt den Management-Blade-Server und den Failover-Management-Blade-Server. Das Blade mit der geringeren Priorität wird zum Management-Blade-Server. Sie müssen auf der Grundlage Ihrer Umgebung bestimmen, welche Bridge-Priorität für die beiden Blades verwendet werden soll.

- Modi "Transparenter Router" und "Expliziter Proxy"

  Der Blade-Server verwendet für die Konfiguration des Management-Blade-Servers und des Failover-Management-Blade-Servers das Virtual Router Redundancy Protocol (VRRP). Der Management-Blade-Server und der Failover-Management-Blade-Server haben unterschiedliche IP-Adressen, aber externe Geräte stellen mithilfe einer virtuellen IP-Adresse eine Verbindung zum Blade-Server her. So können externe Geräte eine Verbindung zum Blade-Server herstellen (unter Verwendung derselben virtuellen IP-Adresse), unabhängig davon, welches physische Blade aktiv ist. Sie müssen:

  - Die virtuelle IP-Adresse für die externen Geräte bestimmen.
  - Die IP-Adressen für den Management-Blade-Server und den Failover-Management-Blade-Server bestimmen.
  - Angeben, welches Blade der Management-Blade-Server sein soll.

Einrichten der Lights-Out-Verwaltung

Gehen Sie wie nachfolgend beschrieben vor, um die Lights-Out-Verwaltung für die Remote-Hardware-Verwaltung des Blade-Servers einzurichten.

Details zum Einrichten und Verwenden der Lights-Out-Verwaltung finden Sie unter *HP Integrated Lights-Out 2 User Guide*.

Vorgehensweise

1. Weisen Sie mit dem Onboard Administrator der integrierten Lights-Out-Software (iLO) jedes Blades eine IP-Adresse zu.
2. Melden Sie sich im HP-Verwaltungssystem an.
3. Weisen Sie dem Blade-Server eine IP-Adresse zu.

Nach der Installation

Stellen Sie nach der Installation des Blade-Servers sicher, dass Ihre Konfiguration ordnungsgemäß funktioniert. Siehe Testen der Konfiguration.

Anschließen und Konfigurieren des Blade-Servers

Der McAfee® Content Security Blade Server Version 5.6 kann mit Ihrem Netzwerk verbunden und in folgenden Modi konfiguriert werden:

- Standardmodus (nicht ausfallsicher)
- Ausfallsicherer Modus

Standardmodus (nicht ausfallsicher)

Im Standardmodus werden für die Verbindung Ihres Blade-Servers mit dem Netzwerk dieselben Komponenten und Prozesse verwendet, die bereits von vorherigen Versionen des McAfee® Content Security Blade Server-Produkts genutzt wurden.

HINWEIS: Im Standardmodus ist Ihr Blade-Server nicht gegen Hardwareausfälle geschützt. Um gegen Hardwareausfälle gewappnet zu sein, sollten Sie in Betracht ziehen, auf Ihrem Blade-Server, nachdem Sie diesen vollständig eingerichtet, konfiguriert und getestet haben, den ausfallsicheren Modus zu aktivieren.

Ausfallsicherer Modus

Mit der Version 5.6 des McAfee® Content Security Blade Server wird für den Blade-Server ein ausfallsicherer Betriebsmodus eingeführt. In diesem Modus werden alle Verbindungen zwischen Ihrem Netzwerk und dem Blade-Server sowie die Verbindungen innerhalb des Blade-Server-Gehäuses so ausgelegt, dass mehrere Pfade verwendet werden können.

Auf diese Weise kann der Ausfall von Serverkomponenten, Netzwerkgeräten oder Verkabelung, die für Weiterleitung des Datenverkehrs zwischen Ihrem Netzwerk und dem Blade-Server verwendet werden, besser verkraftet werden.

Nachdem Sie Ihren Blade-Server für den Standardmodus konfiguriert haben, lesen Sie das Thema Betrieb im ausfallsicheren Modus, das detaillierte Informationen zum Wechsel in den ausfallsicheren Modus enthält.

Inhalt

- Upgrades von früheren Versionen
- Standardinstallation
- Installieren der Software
- Verwenden der Konfigurationskonsole

Upgrades von früheren Versionen

In den folgenden Themen wird ein Upgrade eines vorhandenen McAfee® Content Security Blade Server auf die Version 5.6 der Software beschrieben.

Falls Sie den ausfallsicheren Modus verwenden möchten, müssen Sie die Interconnect-Module im Blade-Server physisch neu konfigurieren.

VORSICHT: Zum Upgrade früherer Versionen auf McAfee Content Security Blade Server Version 5.6 müssen Sie Zeit für einen Netzwerkausfall vorsehen, da der Blade-Server während des Upgrades keinen Datenverkehr scannt.

HINWEIS: Bevor Sie ein Upgrade der Software Ihres Management- und Failover-Management-Blade-Servers durchführen, lesen Sie Konfigurieren der Interconnect-Module bei der Aktualisierung von einer älteren Version und – falls Sie den ausfallsicheren Modus verwenden möchten – Nutzung der Hardware im ausfallsicheren Modus.

Schritt		Beschreibung
1.	Sichern Sie die vorhandene Konfiguration.	Sichern der vorhandenen Konfiguration
2.	Fahren Sie alle Scan-Blades herunter.	Herunterfahren der Scan-Blades
3.	Fahren Sie beide Management-Blade-Server herunter.	Herunterfahren der Management-Blade-Server
4.	Führen Sie ein Upgrade der Software auf beiden Management-Blade-Servern durch.	Upgrade der Software für den Management-Blade-Server
5.	Installieren Sie die Scan-Blades neu.	Erneute Installation der Scan-Blades
6.	Konfigurieren Sie den ausfallsicheren Modus (sofern erforderlich).	Entscheidung treffen zur Verwendung des ausfallsicheren Modus Aktivieren des ausfallsicheren Modus

Inhalt

- Anschließen und Konfigurieren des Blade-Servers
- Konfigurieren der Interconnect-Module bei der Aktualisierung von einer älteren Version
- Sichern der vorhandenen Konfiguration
- Herunterfahren der Scan-Blades
- Herunterfahren der Management-Blade-Server
- Upgrade der Software für den Management-Blade-Server
- Erneute Installation der Scan-Blades

Konfigurieren der Interconnect-Module bei der Aktualisierung von einer älteren Version

In McAfee® Content Security Blade Server Version 5.6 wurden einige Änderungen an der Art und Weise vorgenommen, wie der Blade-Server die Hardware, insbesondere die Interconnect-Module im Blade-Gehäuse, verwendet.

Frühere Versionen von McAfee® Content Security Blade Server verwendeten zwei Interconnect-Module, Interconnect-Modul 1 für LAN1 und Interconnect-Modul 2 für LAN2.

Die mit Version 5.6 gelieferte Hardware verwendet:

- Im Standardmodus (nicht ausfallsicher) Interconnect-Modul 1 für LAN1 und Interconnect-Modul 3 für LAN2
- Im ausfallsicheren Modus die Interconnect-Module 1 und 2 für LAN1 sowie die Interconnect-Module 3 und 4 für LAN2

Weitere Informationen hierzu finden Sie unter Nutzung der Hardware im ausfallsicheren Modus.

Wenn Sie die Software auf der Hardware einer älteren Version aktualisieren, verwendet Version 5.6 in einer Konfiguration für den Standardmodus weiterhin die Interconnect-Module der vorherigen Version (Interconnect-Modul 1 für LAN1 und Interconnect-Modul 2 für LAN2).

Falls Sie jedoch den ausfallsicheren Modus verwenden möchten, müssen Sie Ihre Netzwerkinfrastruktur neu konfigurieren, um die Interconnect-Module wie unter Installieren der Interconnect-Module für den ausfallsicheren Modus beschrieben zu verwenden.

▸ Upgrades von früheren Versionen

Sichern der vorhandenen Konfiguration

Gehen Sie wie nachfolgend beschrieben vor, um die vorhandene Konfiguration Ihres McAfee® Content Security Blade Servers zu sichern. Es hat sich bewährt, eine vollständige Sicherung Ihrer Blade-Server-Konfiguration zu erstellen, bevor Sie eine Aktualisierung durchführen, auch dann, wenn Sie vorhaben, eine der Aktualisierungsoptionen zu verwenden, die eine Sicherung und Wiederherstellung Ihrer Konfiguration einschließen.

Vorgehensweise

1. Navigieren Sie in der Benutzeroberfläche zu **System | Cluster-Verwaltung | Konfiguration sichern und wiederherstellen**.
2. Wählen Sie die optionalen Elemente aus, die Sie in die Sicherung aufnehmen möchten (versionsabhängig).
   McAfee empfiehlt, vor der Aktualisierung Ihres Blade-Servers alle Optionen zu sichern.
3. Klicken Sie auf **Konfiguration sichern**.
4. Nach kurzer Zeit wird ein Dialogfeld angezeigt, in dem Sie die gesicherte Konfigurationsdatei auf Ihren lokalen Computer herunterladen können.

▸ Aktivieren des ausfallsicheren Modus
▸ Upgrades von früheren Versionen

Herunterfahren der Scan-Blades

Gehen Sie wie nachfolgend beschrieben vor, um die Scan-Blades herunterzufahren.

Vorbereitung

Stellen Sie sicher, dass Sie die Scan-Blades zu einem geeigneten Zeitpunkt herunterfahren, wenn der Netzwerkverkehr am geringsten ist und möglichst wenige Beeinträchtigungen entstehen.

Vorgehensweise

1. Navigieren Sie in der Benutzeroberfläche des Management-Blade-Servers zu **System | Cluster-Verwaltung | Lastenausgleich**.
2. Geben Sie das Administratorkennwort in das Textfeld ein.
3. Klicken Sie neben dem Scan-Blade, das Sie herunterfahren möchten, auf **Herunterfahren**.
4. Sofern erforderlich, wiederholen Sie den Vorgang für andere Scan-Blades, die Sie herunterfahren möchten.

▸ Upgrades von früheren Versionen

Herunterfahren der Management-Blade-Server

Gehen Sie wie nachfolgend beschrieben vor, um den Management-Blade-Server oder den Failover-Management-Blade-Server in Ihrem McAfee® Content Security Blade Server herunterzufahren.

Vorbereitung

Stellen Sie sicher, dass Sie die Management-Blade-Server zu einem geeigneten Zeitpunkt herunterfahren, wenn der Netzwerkverkehr am geringsten ist und möglichst wenige Beeinträchtigungen entstehen.

Vorgehensweise

1. Navigieren Sie in der Benutzeroberfläche des Management-Blade-Servers oder Failover-Management-Blade-Servers, den Sie herunterfahren möchten, zu **System | Appliance-Verwaltung | Systemverwaltung**.
2. Geben Sie Ihr Kennwort in das Textfeld neben **Appliance beenden** ein.
3. Klicken Sie auf **Appliance beenden**.
4. Sofern erforderlich, wiederholen Sie den Vorgang für den verbleibenden Management-Blade-Server.

▸ Upgrades von früheren Versionen

Upgrade der Software für den Management-Blade-Server

Gehen Sie wie nachfolgend beschrieben vor, um die McAfee® Content Security Blade Server-Software zu aktualisieren, die auf dem Management-Blade-Server und dem Failover-Management-Blade-Server installiert ist.

Wenn Sie bei einem vorhandenen McAfee® Content Security Blade Server ein Software-Upgrade auf die neueste Version durchführen, stellen Sie sicher, dass die Software nicht nur auf dem Management-Blade-Server, sondern auch auf dem Failover-Management-Blade-Server aktualisiert wird.

Sie können wählen, auf welche Weise die Blade-Server-Software aktualisiert werden soll:

- Vollständige Installation ausführen und dabei vorhandene Daten überschreiben
- Software unter Beibehaltung der Konfiguration und der E-Mail-Nachrichten installieren
- Software nur unter Beibehaltung der Netzwerkkonfiguration installieren
- Software nur unter Beibehaltung der Konfiguration installieren

HINWEIS: Aufgrund einer Änderung der Architektur in Version 5.6 der Software müssen Sie sicherstellen, dass bei der Verwendung einer Aktualisierungsmethode, die die Konfiguration der vorherigen Version übernimmt, die **Cluster-Kennung** einen Wert zwischen 0 und 255 erhält. Sie finden diese Einstellung unter **System | Cluster-Verwaltung | Lastenausgleich | Cluster-Modus | Cluster-Kennung**.

Vorbereitung

Stellen Sie sicher, dass Sie mit dem integrierten Lights-Out-Modul von HP vertraut sind. Weitere Informationen hierzu finden Sie im HP Integrated Lights-Out User Guide.

Vorgehensweise

1. Fahren Sie den Management-Blade-Server, der aktualisiert werden soll, herunter.

2 Legen Sie die CD-ROM mit der Software E-Mail and Web Security v5.6 ein.
   - Legen Sie die CD-ROM bei einem M3-Gehäuse in das eingebaute CD-ROM-Laufwerk ein.
   - Schließen Sie bei einem M7-Gehäuse das externe CD-ROM-Laufwerk an den Management-Blade-Server, der aktualisiert werden soll, an. Legen Sie anschließend die CD-ROM in das CD-ROM-Laufwerk ein.
3 Stellen Sie von einem Computer, auf dem die integrierte Lights-Out-Funktion läuft, eine Verbindung zu dem Gehäuse her.
4 Wählen Sie in der integrierten Lights-Out-Konsole den Management-Blade-Server aus.

   HINWEIS: Der Management-Blade-Server befindet sich in Steckplatz 1 und der Failover-Management-Blade-Server in Steckplatz 2 des Gehäuses.

5 Wählen Sie die Registerkarte **Boot Options** (Startoptionen).

   HINWEIS: Sie können die Software auch von einem USB-Laufwerk aus installieren, das entweder am Blade bzw. am Gehäuse oder an dem Computer angeschlossen sein kann, auf dem die integrierte Lights-Out-Funktion läuft.

6 Überprüfen Sie, ob **CD-ROM** in der Boot-Liste als erstes Gerät aufgeführt ist.
7 Wählen Sie die Registerkarte **Virtual Devices** (Virtuelle Geräte).
8 Klicken Sie auf **Momentary Press** (Kurz drücken), um den Management-Blade-Server von der CD-ROM zu starten.
9 Wählen Sie anhand der Eingabeaufforderungen die gewünschte Aktualisierungsoption und anschließend die zu installierenden Software-Images aus.

   HINWEIS: Wenn Sie **Software unter Beibehaltung der Konfiguration und der E-Mail-Nachrichten installieren** auswählen, wird auf Ihrem Blade-Server die vorhandene Partitionsstruktur wieder in Kraft gesetzt. Das hat zur Folge, dass keine Rescue-Partition erstellt wird. Bei der Verwendung von **Software nur unter Beibehaltung der Netzwerkkonfiguration installieren** oder **Software nur unter Beibehaltung der Konfiguration installieren** wird eine Rescue-Partition erstellt.

▸ Upgrades von früheren Versionen

Erneute Installation der Scan-Blades

Gehen Sie wie nachfolgend beschrieben vor, um die Scan-Blades in Ihrem McAfee® Content Security Blade Server erneut zu installieren.

Vorbereitung

Stellen Sie sicher, dass Sie mit dem integrierten Lights-Out-Modul von HP vertraut sind. Weitere Informationen hierzu finden Sie im HP Integrated Lights-Out User Guide.

Vorgehensweise

1 Wählen Sie mithilfe der Benutzeroberfläche des integrierten Lights-Out-Moduls von HP das Scan-Blade aus, das erneut installiert werden soll.
2 Wählen Sie die Registerkarte **Boot Options** (Startoptionen).
3 Wählen Sie aus der Dropdown-Liste **One Time Boot from:** (Einmalig Starten von) die Option **PXE NIC** **.

4 Klicken Sie auf **Übernehmen**.

5 Wählen Sie die Registerkarte **Virtual Devices** (Virtuelle Geräte).

6 Klicken Sie auf **Momentary Press** (Kurz drücken), um das Scan-Blade von dem Image zu starten, das auf dem Management-Blade-Server gespeichert ist.

7 Wiederholen Sie diese Schritte für jedes Scan-Blade, das erneut installiert wird.

▸ Upgrades von früheren Versionen

Standardinstallation

Die folgende Tabelle enthält einen Überblick über die Installation Ihres McAfee® Content Security Blade Servers Version 5.6.

Die Tabelle enthält auch die ersten Schritte, wenn Sie Ihren Blade-Server im ausfallsicheren Modus installieren möchten.

Schritt		Beschreibung
1.	Packen Sie alle Komponenten aus, und prüfen Sie den Inhalt anhand der Packlisten in der Kiste.	Packlisten
2.	Montieren Sie das Gehäuse im Rack, und installieren Sie den OA und alle Interconnect-Module.	Montieren des Blade-Servers Installieren der Interconnect-Module **Siehe auch** HP BladeSystem c3000 Enclosure Quick Setup Instructions oder HP BladeSystem c7000 Enclosure Quick Setup Instructions HP BladeSystem c3000 Enclosure Setup and Installation Guide oder HP BladeSystem c7000 Enclosure Setup and Installation Guide HP Integrated Lights-Out User Guide
3.	Schließen Sie die Peripheriegeräte und die Stromversorgung an.	Anschließen des Blade-Servers an das Stromnetz **Siehe auch** HP BladeSystem c3000 Enclosure Quick Setup Instructions oder HP BladeSystem c7000 Enclosure Quick Setup Instructions HP BladeSystem c3000 Enclosure Setup and Installation Guide oder HP BladeSystem c7000 Enclosure Setup and Installation Guide HP Integrated Lights-Out User Guide
4.	Schließen Sie den Blade-Server an das Netzwerk an.	Verbindung mit dem Netzwerk
5.	Installieren Sie die Software auf den Management-Blade-Servern.	Installieren der Software
6.	Führen Sie die grundlegende Konfiguration durch.	Verwenden der Konfigurationskonsole
7.	Wählen Sie die zu installierende Software aus.	Software-Images
8.	Installieren Sie die Blade-Server zum Scannen von Inhalten nacheinander, und führen Sie einen PXE-Start des Management-Blade-Servers aus.	Installieren der Software auf einem Blade-Server zum Scannen von Inhalten
9.	Leiten Sie den Testnetzwerkverkehr durch den Blade-Server.	Testen der Konfiguration

Schritt	Beschreibung
10. Testen Sie, ob der Netzwerkverkehr gescannt wird.	Testen der Konfiguration
11. Konfigurieren Sie Richtlinien und Berichte.	Verwenden von Richtlinien für die Verwaltung von Nachrichten-Scans
12. Konfigurieren Sie den Produktionsverkehr durch das System.	Verwenden der Konfigurationskonsole

VORSICHT: Wenn Sie den Blade-Server an Ihr Netzwerk anschließen, können der Internetzugang oder andere Netzwerkdienste unterbrochen werden. Planen Sie einen Zeitraum ein, in dem das Netzwerk nicht verfügbar ist, vorzugsweise zu einer Zeit mit geringer Netzwerkauslastung.

Inhalt

- Anschließen und Konfigurieren des Blade-Servers
- Montieren des Blade-Servers
- Installieren der Interconnect-Module
- Anschließen des Blade-Servers an das Stromnetz
- Verbindung mit dem Netzwerk

Montieren des Blade-Servers

HINWEIS: Weitere Informationen über Demontage und Montage der Blade-Gehäuse und -Komponenten finden Sie für M3-Gehäuse in HP BladeSystem c3000 Enclosure Quick Setup Instructions und HP BladeSystem c3000 Enclosure Setup and Installation Guide und für M7-Gehäuse in HP BladeSystem c7000 Enclosure Quick Setup Instructions und HP BladeSystem c7000 Enclosure Setup and Installation Guide.

Gehen Sie wie nachfolgend beschrieben vor, um den Blade-Server zu montieren.

Vorgehensweise

1. Nehmen Sie den Blade-Server aus der Schutzverpackung, und legen Sie ihn auf eine ebene Fläche.

   TIPP: Aufgrund seines Gewichts sollten Sie den Blade-Server so nah wie möglich am vorgesehenen Installationsort auspacken.

2. Entfernen Sie die vorderen und hinteren Komponenten sowie den hinteren Käfig des Blade-Servers.
3. Montieren Sie den hinteren Käfig, die Netzteile, die Kühllüfter, die Interconnect-Module und die Onboard Administrator-Komponenten erneut.

   TIPP: McAfee empfiehlt, alle Stromversorgungen und Kühllüfter zu montieren und zu nutzen, um beim Ausfall einer Stromversorgungseinheit Redundanz zu gewährleisten.

4. Schließen Sie einen Monitor und eine Tastatur an den Blade-Server an.
5. Verbinden Sie die Netzkabel mit dem Monitor und dem Blade-Server, schließen Sie sie jedoch noch nicht an die Spannungsversorgung an.

Installieren der Interconnect-Module

Bevor Sie Verbindungen aufbauen, müssen Sie die Ethernet-Interconnect-Module installieren und konfigurieren.

Tabelle 1: Legende zu den Abbildungen 9 und 10

#	Beschreibung
1	Anschlüsse für Stromversorgung
2	Interconnect-Modul 1 (verbindet mit LAN 1)
3	Interconnect-Modul 3 (verbindet mit LAN 2) (Beim Upgrade einer älteren Version vorhandener Hardware siehe Konfigurieren der Interconnect-Module bei der Aktualisierung von einer älteren Version.)
4	Onboard-Administrator-Anschluss
5	Onboard-Administrator-Modul
6	Out-of-Band-Zugang (Anschluss 20) (Ist erst aktiviert, nachdem die Interconnect-Module konfiguriert wurden.)

M3-Gehäuse

Beim M3-Gehäuse werden die Interconnect-Module an der Rückseite des Gehäuses installiert.

Das Interconnect-Modul LAN 1 wird in das obere linke Interconnect-Modul-Fach eingesetzt, das Interconnect-Modul LAN 2 in das obere rechte Interconnect-Modul-Fach.

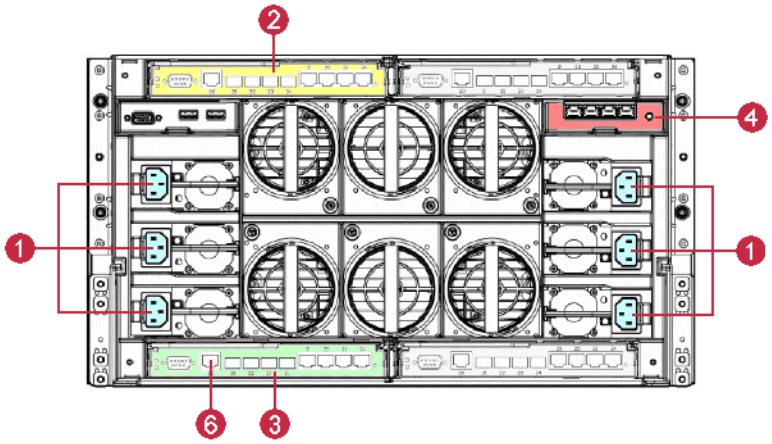


Abbildung 9: M3-Gehäuse – Positionen der Komponenten auf der Rückseite – Standardmodus (nicht ausfallsicher)

M7-Gehäuse

Beim M7-Gehäuse werden die Interconnect-Module an der Rückseite des Gehäuses direkt unter der oberen Kühllüfterreihe installiert.

Das Interconnect-Modul LAN 1 wird in das obere linke Interconnect-Modul-Fach eingesetzt, das Interconnect-Modul LAN 2 direkt darunter in das untere linke Interconnect-Modul-Fach.

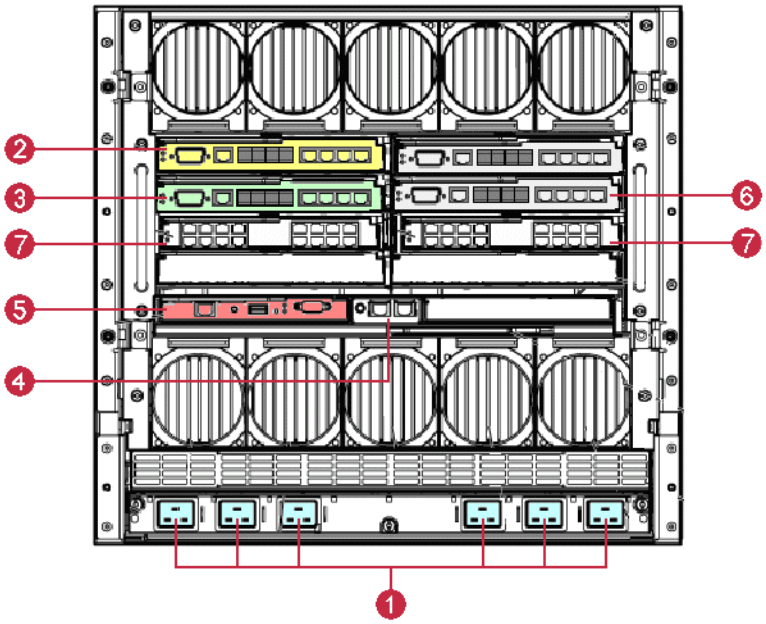


Abbildung 10: M7-Gehäuse – Positionen der Komponenten auf der Rückseite – Standardmodus (nicht ausfallsicher)

Führen Sie Folgendes aus:

- Deaktivieren Sie STP (Spanning Tree Protocol) für die STP-Gruppe 1 (standardmäßig sind alle Anschlüsse Mitglieder der STP-Gruppe 1). (Dies gilt, wenn Sie den Blade-Server im Modus "Transparente Bridge" installieren.)
- Konfigurieren Sie die ACLs (Access Control Lists, Zugriffssteuerungslisten) auf den Interconnect-Modulen so, dass die Blade-Server zum Scannen von Inhalten keine externen DHCP-Adressen empfangen können.
- Konfigurieren Sie die ACLs so, dass die Blade-Heartbeat-Pakete im Blade-Server verbleiben.
- Wenn für ein VLAN gekennzeichneter Datenverkehr durch den Blade-Server geleitet werden soll, müssen die Interconnect-Module so konfiguriert werden, dass sie diesen Datenverkehr durchlassen.

Informationen dazu, wie Sie dies tun, finden Sie in der unten aufgeführten Dokumentation:

- HP GbE2c Layer 2/3 Ethernet Blade Switch for c-Class BladeSystem Quick Setup
- HP GbE2c Layer 2/3 Ethernet Blade Switch for c-Class BladeSystem User Guide

HINWEIS: Wenn Sie planen, den Blade-Server zu einem späteren Zeitpunkt für den Betrieb im ausfallsicheren Modus zu konfigurieren, sollten Sie in Erwägung ziehen, die erforderlichen Interconnect-Module bereits jetzt zu installieren. Anweisungen hierzu finden Sie unter Installieren der Interconnect-Module für den ausfallsicheren Modus.

▸ Standardinstallation

Anschließen des Blade-Servers an das Stromnetz

Gehen Sie wie nachfolgend beschrieben vor, um den Blade-Server an das Stromnetz anzuschließen und einzuschalten.

Vorgehensweise

1 Schließen Sie die Netzkabel an die Blade-Netzteile und Stromsteckdosen an.

HINWEISE

- Um sicherzustellen, dass alle Blades mit Strom versorgt sind, verwenden Sie zwei unterschiedliche Stromkreise. *Wenn nur ein Stromkreis verwendet wird und die Einstellungen für die Stromversorgung für "Wechselstrom - redundant" konfiguriert sind (wie empfohlen), können einige Blades nicht hochgefahren werden.*
- Falls die Netzkabel für das Einsatzland nicht geeignet sind, setzen Sie sich mit Ihrem Händler in Verbindung.

2 Schalten Sie den Blade-Server ein, indem Sie die Netzschalter am Management-Blade-Server und am Failover-Management-Blade-Server drücken.

▸ Standardinstallation

Verbindung mit dem Netzwerk

Welche Interconnect-Module und Kabel Sie verwenden, um den Blade-Server an Ihr Netzwerk anzuschließen, hängt vom Netzwerkmodus ab, den Sie für den Blade-Server gewählt haben. Informationen zu Netzwerkmodi finden Sie unter Überlegungen zu Netzwerkmodi.

HINWEIS: Wenn Sie ein Upgrade von einer früheren Version mit einer vorhandenen Hardware durchführen, finden Sie unter Konfigurieren der Interconnect-Module bei der Aktualisierung von einer älteren Version weitere Informationen darüber, welche Netzwerkverbindungen verwendet werden müssen.

Im Standardmodus sind die folgenden Verbindungen zwischen Ihrem Blade-Server und den Netzwerk-Switches erforderlich:

- **Modus "Transparente Bridge"** – Der Blade-Server fungiert als Bridge zwischen zwei Netzwerksegmenten. Schließen Sie das Interconnect-Modul 1 (LAN1) an ein Segment und das Interconnect-Modul 3 (LAN2) an das andere Segment an. Verwenden Sie dazu Kabel, die an einen der Anschlüsse 21-24 jedes Interconnect-Moduls angeschlossen sind. Die Verbindung zur Out-of-band-Verwaltung kann über einen anderen der LAN2-Anschlüsse hergestellt und konfiguriert werden.
- **Modus "Transparenter Router"** – Der Blade-Server fungiert als Router, der zwei separate Netzwerke miteinander verbindet. Schließen Sie das Interconnect-Modul 1 (LAN1) an ein Netzwerk und das Interconnect-Modul 3 (LAN2) an das andere Netzwerk an. Verwenden Sie dazu Kabel, die an einen der Anschlüsse 21-24 jedes Interconnect-Moduls angeschlossen sind. Die Verbindung zur Out-of-band-Verwaltung kann über einen anderen der LAN2-Anschlüsse hergestellt und konfiguriert werden.
- **Modus "Expliziter Proxy"** – Es wird eine einzelne Verbindung zwischen Interconnect-Modul 3 (LAN2) und Ihrem Netzwerk benötigt. (Bei Systemen, bei denen ein Upgrade durchgeführt wurde, wird LAN2 über das Interconnect-Modul 2 angeschlossen.) LAN1 kann für den Anschluss des Netzwerks verwendet werden, jedoch wird die maximale Leistung erreicht, wenn LAN1 für das Scanning-Netzwerk innerhalb des Blade-Servers verwendet wird. (Diese Einschränkung gilt nicht im ausfallsicheren Modus.)

Verwenden von Kupfer-LAN-Verbindungen

Verwenden Sie die Interconnect-Module LAN1 und LAN2 sowie die im Lieferumfang enthaltenen Netzwerkkabel (oder entsprechende Cat-5e- bzw. Cat-6-Ethernet-Kabel), und schließen Sie den Blade-Server entsprechend dem gewählten Netzwerkmodus an Ihr Netzwerk an.

Modus "Transparente Bridge"

Schließen Sie die Interconnect-Module LAN1 und LAN2 des Blade-Servers mit den mitgelieferten Kupfer-LAN-Kabeln an Ihr Netzwerk an, um den Blade-Server in den Datenstrom einzufügen.

Modus "Transparenter Router"

Der Blade-Server fungiert als Router. Die LAN-Segmente, die mit den beiden Netzwerkschnittstellen verbunden sind, müssen sich deshalb in verschiedenen IP-Subnetzen befinden. Das Gerät muss einen bestehenden Router ersetzen, oder auf der Seite des Blade-Servers muss ein neues Subnetz angelegt werden. Ändern Sie hierfür die IP-Adresse oder die Netzmaske, die die Computer auf dieser Seite verwenden.

Modus "Expliziter Proxy"

Schließen Sie das Interconnect-Modul LAN2 mit einem Kupfer-LAN-Kabel (mitgeliefert) an das Netzwerk an. Bei diesem Kabel handelt es sich um ein durchgängiges (ungekreuztes) Kabel, das den Blade-Server mit einem normalen, ungekreuzten RJ-45-Netzwerkanschluss verbindet.

LAN1 kann für den Anschluss des Netzwerks verwendet werden, jedoch wird die maximale Leistung erreicht, wenn LAN1 für das Scanning-Netzwerk innerhalb des Blade-Servers verwendet wird. (Diese Einschränkung gilt nicht im ausfallsicheren Modus.)

Verwenden von Glasfaser-LAN-Verbindungen

Bevor Sie Verbindungen herstellen, müssen Sie die Glasfaseroptik-SFP-Transceiver (Small Form-Factor Pluggable) installieren. Anweisungen dazu finden Sie unter HP GbE2c Layer 2/3 Ethernet Blade Switch for c-Class BladeSystem.

HINWEIS: Verwenden Sie ausschließlich Glasfaseroptik-SFP-Transceiver von HP oder McAfee. Wenn Sie SFP-Transceiver anderer Hersteller verwenden, ist wahrscheinlich kein Zugriff auf den Blade-Server möglich.

Schließen Sie die Interconnect-Module LAN1 und LAN2 mit Glasfaserkabeln an das Netzwerk an. Welche Interconnect-Module und Kabel Sie verwenden, hängt vom Betriebsmodus des Blade-Servers ab.

Modus "Transparente Bridge"

Schließen Sie die Interconnect-Module LAN1 und LAN2 mit Glasfaserkabeln an das Netzwerk an.

Modus "Transparenter Router"

Schließen Sie die Interconnect-Module LAN1 und LAN2 mit Glasfaserkabeln an verschiedene IP-Subnetze an.

Modus "Expliziter Proxy"

Schließen Sie das Interconnect-Modul LAN2 mit einem Glasfaser-LAN-Kabel (mitgeliefert) an das Netzwerk an.

LAN1 kann für den Anschluss des Netzwerks verwendet werden, jedoch wird die maximale Leistung erreicht, wenn LAN1 für das Scanning-Netzwerk innerhalb des Blade-Servers verwendet wird. (Diese Einschränkung gilt nicht im ausfallsicheren Modus.)

Installieren der Software

Gehen Sie wie nachfolgend beschrieben vor, um die Blade-Server-Software auf dem Management-Blade-Server und dem Failover-Management-Blade-Server zu installieren.

Vorgehensweise

- Anschließen und Konfigurieren des Blade-Servers
- Installationsreihenfolge der Management-Blade-Server
- Software-Images
- Installieren der Software auf einem Blade-Server zum Scannen von Inhalten

Installationsreihenfolge der Management-Blade-Server

Installieren Sie den Management-Blade-Server und den Failover-Management-Blade-Server in den Steckplätzen 1 und 2 des Blade-Server-Gehäuses.

Verbinden Sie beide Management-Blades gemäß den Anweisungen unter Installation der Software auf den Management-Blade-Servern, und installieren Sie die Software.

Wenn Sie beide Management-Blade-Server gleichzeitig konfigurieren, sparen Sie nicht nur Zeit, sondern verhindern auch, dass dem zweiten Management-Blade-Server eine IP-Adresse im Scanning-Netzwerk zugewiesen wird, wenn der DHCP-Server des ersten Management-Blade-Servers gestartet wird.

- Installieren der Software

Software-Images

In Content Security Blade Server 5.6 können Sie die Software-Images auswählen, die auf den Blade-Servern zum Scannen von Inhalten installiert werden können. Folgende Optionen stehen zur Auswahl:

- Email and Web Security
- Email Security
- Web Security
- McAfee Web Gateway (vormals WebWasher)

Wenn Sie Email and Web Security auswählen, wird dieses Software-Image auf allen Blade-Servern zum Scannen von Inhalten installiert. Wenn Sie Email Security und entweder Web Security oder McAfee Web Gateway auswählen, konfigurieren Sie jeden Blade-Server zum Scannen von Inhalten so, dass er entweder E-Mail-Verkehr oder Web-Verkehr scannt.

HINWEIS: Sie können entweder Web Security oder McAfee Web Gateway auswählen. Sie können nicht beide Web-Scan-Images auf demselben Blade-System installieren.

Weitere Informationen zum Konfigurieren der McAfee Web Gateway-Software finden Sie im *Installations- und Konfigurationshandbuch für McAfee Web Gateway-Appliances*.

- Installieren der Software
- Installation der Software auf den Management-Blade-Servern
- Synchronisierung von Konfigurationsänderungen

Installation der Software auf den Management-Blade-Servern

Gehen Sie wie nachfolgend beschrieben vor, um die Software auf dem Management-Blade-Server oder dem Failover-Management-Blade-Server zu installieren.

Sie können die Software lokal auf dem Blade-Server installieren oder remote unter Verwendung der integrierten Lights-Out-Funktion. Die integrierte Lights-Out-Funktion stellt Einrichtungen für virtuelle Medien zur Verfügung, die Sie für das Remote-Mounten eines physischen CD-ROM-Laufwerks, einer ISO-Image-Datei oder eines USB-Laufwerks verwenden können, die die Installationsinformationen enthalten.

Vorbereitung

Sehen Sie nach, ob auf der McAfee-Download-Seite neuere Versionen Ihrer Software erhältlich sind:

http://www.mcafee.com/us/downloads/

HINWEIS: Sie benötigen hierfür eine gültige Grant-Nummer.

Vorgehensweise

1. Setzen Sie den Management-Blade-Server in Position 1 (für den Management-Blade-Server) oder Position 2 (für den Failover-Management-Blade-Server) ein.
2. Schließen Sie Folgendes an den Blade-Server an:
   - Schließen Sie bei einem M3-Gehäuse einen Monitor und eine Tastatur an das KVM-Modul auf der Rückseite des Chassis an. Mounten Sie mithilfe der KVM-Schnittstelle das CD/DVD-ROM-Laufwerk auf dem Management-Blade-Server, der installiert wird.
   - Schließen Sie bei einem M7-Gehäuse über das mitgelieferte Kabel einen Monitor, eine Tastatur und ein USB-CD-ROM-Laufwerk an den weiterleitenden Konnektor des Management-Blade-Servers oder des Failover-Management-Blade-Servers an.
   - Bei einer Remote-Installation greifen Sie auf die integrierten Lights-Out-Module zu, indem Sie über den Onboard Administrator eine Remote-KVM-Sitzung aufbauen.
3. Starten Sie den Management-Blade-Server oder den Failover-Management-Blade-Server von der Installations- und Wiederherstellungs-CD. Die Software wird auf dem ausgewählten Blade installiert.
4. Legen Sie die grundlegende Konfiguration fest. Siehe Verwenden der Konfigurationskonsole.

▸ Software-Images

Synchronisierung von Konfigurationsänderungen

Alle Änderungen, die Sie auf dem Management-Blade-Server an der Konfiguration vornehmen, werden automatisch mit dem Failover-Management-Blade-Server und den Blade-Servern zum Scannen von Inhalten synchronisiert.

Prüfen Sie auf dem **Dashboard** den Status des Management- und des Failover-Management-Blade-Servers, um sicherzustellen, dass die Synchronisierung stattgefunden hat.

Installieren der Software auf einem Blade-Server zum Scannen von Inhalten

Gehen Sie wie nachfolgend beschrieben vor, um auf einem Blade-Server zum Scannen von Inhalten die Software zu installieren.

Vorgehensweise

1. Wählen Sie in der Benutzeroberfläche die Option **Dashboard**. Unten auf der Seite wird **Blade-Status** angezeigt.
2. Setzen Sie den Blade-Server zum Scannen von Inhalten in das Gehäuse ein. Das Blade wird auf der Seite **Blade-Status** mit dem Status **INSTALLIEREN** angezeigt.
   Die Software wird vom Management-Blade-Server automatisch auf dem Blade-Server zum Scannen von Inhalten installiert. Dieser Vorgang dauert etwa 10 Minuten.
3. Die Daten werden automatisch aktualisiert.
   Nach einigen Minuten ändert sich der Status in **BOOT**, anschließend in **SYNC** und dann in **OK**.

Der neue Blade-Server zum Scannen von Inhalten ist nun funktionsbereit.

▸ Installieren der Software

Verwenden der Konfigurationskonsole

Mit der Software der Version 5.6 wurde der Konfigurationsprozess vereinfacht. Sie können Ihr Gerät jetzt entweder von der Konfigurationskonsole aus oder innerhalb der Benutzeroberfläche mit dem Setup-Assistenten konfigurieren.

Die Konfigurationskonsole wird am Ende der Startsequenz automatisch gestartet, entweder nachdem:

- ein unkonfiguriertes Gerät gestartet wurde
- oder nachdem ein Gerät auf seine Werkseinstellungen zurückgesetzt wurde.

Wird die Konfigurationskonsole gestartet, bietet Sie Ihnen die Möglichkeit, Ihr Gerät von der Gerätekonsole aus in Ihrer bevorzugten Sprache zu konfigurieren, bzw. liefert Anweisungen dafür, wie Sie von einem anderen Computer im selben Subnetz aus eine Verbindung mit dem Setup-Assistenten innerhalb der Benutzeroberfläche herstellen können. Beide Methoden bieten Ihnen dieselben Optionen für die Konfiguration Ihres Geräts.

HINWEIS: Von der Konfigurationskonsole aus können Sie eine neue Installation der Blade-Server-Software konfigurieren. Wenn Sie jedoch für die Konfiguration Ihres Blade-Servers eine zuvor gespeicherte Konfigurationsdatei verwenden möchten, müssen Sie sich bei der Benutzeroberfläche des Blade-Servers anmelden und den Setup-Assistenten ausführen (**System | Setup-Assistent**).

Diese Software-Version enthält die automatische Konfiguration mithilfe von DHCP für folgende Parameter:

- Host-Name
- Domänenname
- Standard-Gateway
- DNS-Server
- Geleaste IP-Adresse

- NTP-Server

▸ Anschließen und Konfigurieren des Blade-Servers
▸ Begrüßungsseite
▸ Durchführen der benutzerdefinierten Einrichtung
▸ Wiederherstellung aus einer Datei

Begrüßungsseite

Dies ist die erste Seite des Setup-Assistenten. Wählen Sie **Benutzerdefinierte Einrichtung**, um Ihren Blade-Server zu konfigurieren, oder **Aus Datei wiederherstellen**, um eine zuvor gespeicherte Blade-Server-Konfiguration wiederherzustellen.

HINWEIS: Wenn Sie über den Setup-Assistenten auf diese Seite zugreifen, werden Sie zur Eingabe Ihres Benutzernamens und Kennworts aufgefordert.

Durchführen der benutzerdefinierten Einrichtung

Bei der benutzerdefinierten Einrichtung enthält der Assistent die folgenden Seiten:

- Datenverkehr
- Grundlegende Einstellungen
- Netzwerkeinstellungen
- Cluster-Verwaltung
- DNS und Routing
- Zeiteinstellungen
- Kennwort
- Zusammenfassung

Datenverkehr

Über diese Seite können Sie den Typ von Datenverkehr angeben, den das Gerät scannt.

- Web-Verkehr umfasst HTTP (für Web-Browsing), ICAP (zur Verwendung mit ICAP-Clients) und FTP für die Dateiübertragung.
- Der E-Mail-Verkehr umfasst SMTP und POP3.

Sie können die einzelnen Protokolle (SMTP, POP3, HTTP, ICAP und FTP) aktivieren oder deaktivieren. Wenn sich das Gerät im Modus "Transparenter Router" oder "Transparente Bridge" befindet und ein Protokoll deaktiviert wird, passiert der Datenverkehr des jeweiligen Protokolls das Gerät, wird aber nicht gescannt.

HINWEIS: Wenn Sie McAfee Web Gateway-Software installieren, muss das Gerät im Modus "Expliziter Proxy" konfiguriert sein.

Wenn Sie Web Security Gateway verwenden möchten, geben Sie auf dieser Seite die Zeitpläne für Software-Aktualisierungen an, und laden Sie die Lizenzdatei hoch.

Wenn sich das Gerät im Modus "Expliziter Proxy" befindet und ein Protokoll deaktiviert wird, wird der Verkehr abgelehnt, der für dieses Protokoll an den Blade-Server gesendet wird. Das Protokoll wird im Gerät blockiert. Im Modus "Expliziter Proxy" wird nur SMTP-, POP3-, HTTP-, ICAP- und FTP-Verkehr vom Blade-Server verarbeitet. Sämtlicher anderer Datenverkehr wird abgelehnt.

Wenn nach der Installation gar kein Datenverkehr gescannt werden soll, können Sie alle Protokolle auf dieser Seite deaktivieren. Wählen Sie im Menü **E-Mail | E-Mail-Konfiguration | Protokollkonfiguration** oder **Web | Web-Konfiguration**.

Optionsbeschreibungen

Option	Beschreibung	
Web-Verkehr scannen	**Scan-Geräte für McAfee Web Gateway verwenden**	Wählen Sie diese Option aus, um die Software McAfee Web Gateway (früher WebWasher) auf einem oder mehreren Ihrer Blade-Server zum Scannen von Inhalten zu installieren. Weitere Optionen ermöglichen Ihnen Folgendes: • Lizenzdatei für McAfee Web Gateway hochladen • Intervall der URL-Filter-Aktualisierungen festlegen • Intervall der Antiviren-Aktualisierungen für McAfee Web Gateway festlegen • Intervall der Aktualisierungen für das proaktive Scannen festlegen • Intervall der CRL-Aktualisierungen festlegen
	Scan-Geräte für Web Security verwenden	Wählen Sie diese Option aus, um Web Security-Scanning auf Ihrem Blade-Server zu installieren. Sie können auch die Option **Schutz gegen potentiell unerwünschte Programme (einschließlich Spyware) aktivieren** auswählen. McAfee Anti-Spyware schützt Ihr Netzwerk vor vielen Arten potenziell unerwünschter Software, wie Spyware, Adware, Remote-Verwaltungs-Tools, Dialern und Kennwort-Crackern. Diese Funktion ist standardmäßig nicht aktiviert. HINWEIS: McAfee Anti-Spyware wurde dazu entwickelt, potenziell unerwünschte Programme (PUPe) zu erkennen und mit Ihrer Erlaubnis zu entfernen. Manche gekauften oder absichtlich heruntergeladenen Programme agieren als Hosts für potenziell unerwünschte Programme. Wenn diese potenziell unerwünschten Programme entfernt werden, funktionieren ihre Hosts möglicherweise nicht mehr. Genaue Informationen entnehmen Sie bitte dem Lizenzvertrag für das jeweilige Hostprogramm. McAfee, Inc. fordert weder zum Bruch von abgeschlossenen Lizenzverträgen auf, noch duldet es dies. Lesen Sie Lizenzverträge und Datenschutzrichtlinien unbedingt gründlich durch, bevor Sie Software herunterladen oder installieren.
E-Mail-Verkehr scannen	Der E-Mail-Verkehr umfasst SMTP- und POP3-Verkehr. Nach der Installation: Das Gerät schützt Ihr Netzwerk vor Viren, Spam und Phishing und verwendet McAfee TrustedSource, um Ihr Netzwerk vor unerwünschten E-Mails zu schützen. Des Weiteren stehen die folgenden Optionen zur Verfügung: • **Schutz gegen potentiell unerwünschte Programme (einschließlich Spyware) aktivieren** • **SMTP-Verkehr scannen** • **POP3-Verkehr scannen**	
Lokale Relay-Domäne	Unter **Relay-Optionen** schlägt das Gerät die Domäneninformationen vor, sofern diese über DHCP verfügbar sind. Löschen Sie den Stern, wenn Sie den vorgeschlagenen Domänennamen verwenden möchten, oder geben Sie einen anderen Domänennamen ein.	

Grundlegende Einstellungen

Verwenden Sie diese Seite, um grundlegende Einstellungen für den Blade-Server anzugeben.

Der Blade-Server versucht, Ihnen einige Informationen zur Verfügung zu stellen, und zeigt die Informationen gelb markiert an. Um diese Informationen zu ändern, klicken Sie, und geben Sie sie erneut ein.

Optionsbeschreibungen

Option	Beschreibung
Cluster-Modus	• **Cluster-Master** – Dieses Blade wird zum Management-Blade-Server und steuert die Scan-Arbeitslast verschiedener anderer Blade-Server zum Scannen von Inhalten. • **Cluster-Failover** –- Falls der Management-Blade-Server ausfällt, steuert stattdessen dieses Blade die Scan-Arbeit.
Gerätename	Gibt einen Namen an, z. B. Appliance1.
Domänenname	Gibt einen Namen an, z. B. domäne.beispiel.com.
Standard-Gateway (IPv4)	Gibt eine IPv4-Adresse an, z. B. 198.168.10.1. Sie können später testen, ob die Appliance mit diesem Server kommunizieren kann.
Nächster Hop-Router (IPv6)	Gibt eine IPv6-Adresse an, z. B. FD4A:A1B2:C3D4::1.

Netzwerkeinstellungen

Wenn Sie für eine neue Installation zum ersten Mal eine Konfiguration ausführen (oder die Standardeinstellung wiederherstellen), wird die Seite "Netzwerkeinstellungen" angezeigt. Wenn Sie den Cluster-Modus des Geräts ändern, wird diese Seite ebenfalls angezeigt.

Verwenden Sie diese Seite, um die IP-Adresse, die Netzwerkgeschwindigkeiten und den Betriebsmodus für das Gerät zu konfigurieren.

Wenn möglich, füllt das Gerät viele dieser Optionen mithilfe von DHCP aus. Die IP-Adressen müssen eindeutig und für Ihr Netzwerk geeignet sein. Geben Sie nur so viele IP-Adressen wie erforderlich an.

Optionsbeschreibungen

Option	Beschreibung
Netzwerkeinstellungen ändern	Durch Klicken auf diese Option wird ein Assistent mit den folgenden Optionen gestartet.
Betriebsmodus	Bietet eine Auswahl an Modi. Im Modus **Transparenter Router** oder **Transparente Bridge** wissen andere Netzwerkgeräte wie beispielsweise E-Mail-Server nicht, dass der Blade-Server die E-Mail vor dem Weiterleiten abgefangen und gescannt hat. Der Vorgang ist für andere Geräte **transparent**. Im Modus **Expliziter Proxy** senden einige Netzwerkgeräte Datenverkehr an die Appliance. Der Blade-Server fungiert dann als **Proxy** und verarbeitet den Datenverkehr für die Geräte.
LAN-Schnittstellentyp	Gibt den Verbindungstyp an – Kupferleitung oder Glasfaser. Diese Option ist nur für High-Speed-Appliances verfügbar.
IP-Adresse	Gibt Netzwerkadressen an, die es dem Blade-Server ermöglichen, mit Ihrem Netzwerk zu kommunizieren. Beispiel: 198.168.10.1. Geben Sie für jeden Management-Blade-Server die IP-Adresse an.

Option	Beschreibung
	Sie können mehrere IP-Adressen für die Blade-Server-Anschlüsse angeben. Wenn sich der Blade-Server im Modus "Transparente Bridge" befindet, werden die IP-Adressen für beide Anschlüsse in einer Liste zusammengefasst. Klicken Sie in den anderen Modi auf **Netzwerkschnittstelle 1** bzw. **Netzwerkschnittstelle 2**, um die jeweilige Liste zu bearbeiten. Konfigurieren Sie die IP-Adresse für den Management-Blade-Server sowie für den Lastenausgleich. Wenn Sie im Modus "Expliziter Proxy" oder "Transparenter Router" arbeiten, erstellen Sie eine virtuelle IP-Adresse. Die virtuelle IP-Adresse muss für den Management- und den Failover-Management-Blade-Server gleich sein. HINWEIS: Sie müssen für den Failover-Management-Blade-Server sowohl für die physische IP-Adresse als auch für den Lastenausgleich andere IP-Adressen festlegen als für den Management-Blade-Server. Bei der ersten IP-Adresse in der Liste handelt es sich um die primäre Adresse. Bei den nachfolgenden IP-Adressen handelt es sich um Aliasadressen.
Netzwerkmaske	Gibt die IPv4-Netzwerkmaske an, z. B. 255.255.255.0, oder gibt die IPv6-Präfixlänge an (1-64 oder 128).

Cluster-Verwaltung

Mithilfe dieser Seite können Sie die Anforderungen an den Lastenausgleich angeben.

- Cluster-Verwaltung (Cluster-Master)
- Cluster-Verwaltung (Cluster-Failover)

Ein *Cluster* ist eine Gruppe von Geräten, die gemeinsame Konfigurationen haben und den Netzwerkverkehr untereinander aufteilen.

Der Cluster enthält Folgendes:

- Einen *Cluster-Master*. Der Master synchronisiert die Konfiguration und verteilt die Last des Netzwerkverkehrs auf die anderen Cluster-Mitglieder.
- Ein *Cluster-Failover*. Falls der Cluster-Master ausfällt, übernimmt das Cluster-Failover nahtlos die Arbeit des Cluster-Masters.
- Einen oder mehrere *Cluster-Scanner*. Diese scannen den Datenverkehr gemäß den vom Master synchronisierten Richtlinien.

Vorzüge

- Eine skalierbare Leistung aufgrund des Lastenausgleichs zwischen mehreren Geräten macht teure Upgrades überflüssig.
- Eine einfachere Verwaltung durch die Synchronisierung von Konfiguration und Aktualisierungen verringert den Verwaltungsaufwand.
- Eine verbesserte Stabilität durch hohe Verfügbarkeit vermindert das Risiko ungeplanter Ausfälle.
- Verbesserte Analyse durch konsolidierte Berichte.

Einrichten des Clusters

Beim Konfigurieren eines Masters oder Failovers muss der Administrator Folgendes tun:

- Für den Proxy-Modus oder den Modus "Transparenter Router" eine virtuelle IP-Adresse festlegen, die für den Master und das Failover gleich ist. Die Cluster-Mitglieder verwenden dann für ein Failover VRRP.

- Für den Modus "Transparente Bridge" den Cluster zur Verwendung von STP im Fall eines Failovers einrichten. Die Bridge-Priorität muss auf dem Master niedriger sein (standardmäßig eingestellt).

Für alle Cluster-Mitglieder muss der Administrator die *Cluster-Kennung* festlegen. Diese eindeutige Kennung stellt sicher, dass die Mitglieder des Clusters korrekt miteinander verbunden werden. Zum Erstellen mehrerer Cluster können Sie für jeden Cluster eine unterschiedliche Kennung verwenden.

Leiten Sie den gesamten zu scannenden Netzwerkverkehr an den Cluster-Master (oder an die virtuelle IP-Adresse, wenn ein Cluster-Failover verwendet wird).

Verwalten des Clusters

Nachdem der Cluster konfiguriert wurde, wird er automatisch mithilfe der Cluster-Kennung verbunden. Das Dashboard des Cluster-Masters zeigt den Geräte- und den Cluster-Typ an.

Der Administrator muss Verwaltungsaufgaben, wie zum Beispiel das Festlegen von Scan-Richtlinien, anschließend nur in der Benutzeroberfläche des Cluster-Masters ausführen. Der Cluster-Master gibt dann diese Konfiguration automatisch an die anderen Cluster-Mitglieder weiter.

Der Cluster-Master fasst Folgendes zusammen:

- Antiviren-Aktualisierungen
- Berichte
- E-Mail in der Warteschlange
- McAfee Quarantine Manager (MQM)

HINWEIS: Software-Patches müssen auf dem Management-Blade-Server angewendet werden, der diese daraufhin an den Failover-Management-Blade-Server und an die Blade-Server zum Scannen von Inhalten überträgt.

Cluster-Verwaltung (Cluster-Master)

Verwenden Sie diese Seite, um Informationen für den Management-Blade-Server anzugeben.

Option	Beschreibung
Für Lastenausgleich zu verwendende Adresse	Gibt die Adresse des Management-Blade-Servers an.
Cluster-Kennung	Gibt eine ID an. Der Bereich liegt zwischen 0 und 255.

Cluster-Verwaltung (Cluster-Failover)

Verwenden Sie diese Seite, um Informationen für den Failover-Management-Blade-Server anzugeben.

Option	Beschreibung
Für Lastenausgleich zu verwendende Adresse	Gibt die Adresse des Failover-Management-Blade-Servers an. Bietet eine Liste aller einer Appliance zugewiesenen Subnetze.
Cluster-Kennung	Gibt eine ID an. Der Bereich liegt zwischen 0 und 255.

DNS und Routing

Verwenden Sie diese Seite, um die Verwendung von DNS und Routen durch das Gerät zu konfigurieren.

DNS-Server (Domain Name System) übersetzen die Namen von Netzwerkgeräten in IP-Adressen (und umgekehrt), d. h., sie ordnen die Namen und Adressen einander zu. Das Gerät sendet in der hier aufgeführten Reihenfolge Anfragen an DNS-Server.

Optionsbeschreibungen

Option	Beschreibung
Serveradresse	Gibt die DNS-Server an. Beim ersten Server in der Liste muss es sich um den schnellsten bzw. zuverlässigsten Server handeln. Falls der erste Server die Anforderung nicht auflösen kann, nimmt das Gerät Kontakt mit dem zweiten Server auf. Falls keiner der Server in der Liste die Anforderung auflösen kann, leitet das Gerät die Anforderung an die DNS-Root-Namenserver im Internet weiter. Wenn DNS-Suchvorgänge (in der Regel auf Port 53) von der Firewall verhindert werden, geben Sie die IP-Adresse eines lokalen Geräts mit Namensauflösungsfunktion an.
Netzwerkadresse	Zeigt die Netzwerkadresse eines Routing-Geräts an.
Maske	Zeigt die Netzwerk-Subnetzmaske an (beispielsweise 255.255.255.0).
Gateway	Gibt die IP-Adressen der anderen Gateways (typischerweise Firewalls oder Router) an, über die das Gerät mit dem Netzwerk kommuniziert. Die Seite **Grundlegende Einstellungen** gibt das Standard-Gateway an.
Messgröße	Zeigt einen Wert an, der von der Routing-Software verwendet wird. Der Standardwert ist 0.0.
Dynamisches Routing aktivieren	Das dynamische Routing erlaubt es Ihren Netzwerkgeräten, einschließlich des Geräts, die Routing-Informationen abzuhören, die Router in Ihrem Netzwerk per Broadcast verbreiten. Die Geräte können anhand dieser Informationen ihre eigenen Routing-Informationen konfigurieren. HINWEIS: Das Gerät unterstützt nur die Routing-Protokolle Routing Information Protocol (RIP) und Open Shortest Path First (OSPF).

Zeiteinstellungen

Auf dieser Seite können Sie die Uhrzeit und das Datum sowie sämtliche Details für die Verwendung von NTP (Network Time Protocol) festlegen. NTP synchronisiert die Uhrzeiten unter den Geräten in einem Netzwerk. Einige Internet-Dienstanbieter bieten einen Uhrzeitdienst an. Weitere Informationen über NTP finden Sie in RFC 1305 unter www.apps.ietf.org/rfc/rfc1305.html, www.ntp.org oder www.ntp.isc.org.

Das Gerät kann seine Uhrzeiteinstellungen mit anderen Geräten synchronisieren, damit seine eigenen Protokolle, Berichte und Zeitpläne stets genau sind. Da NTP-Nachrichten nicht häufig versendet werden, haben sie keinen merklichen Einfluss auf die Leistung des Blade-Servers.

Optionsbeschreibungen

Option	Beschreibung
Zeitzone	Gibt Ihre lokale Zeitzone an. Wenn in Ihrer Region Sommer- und Winterzeit gelten, müssen Sie die Zeitzone zweimal im Jahr ändern.
Systemzeit (lokal)	Gibt das Datum und die lokale Uhrzeit an. Klicken Sie auf das Kalendersymbol, um das Datum festzulegen.

Option	Beschreibung
Uhrzeit jetzt einstellen	Wenn Sie darauf klicken, wird die Zeit im Gerät eingestellt. Sie müssen auf diese Schaltfläche klicken, bevor Sie auf **Weiter** klicken. Falls erforderlich, können Sie nach der Installation NTP (Network Time Protocol) konfigurieren.
NTP aktivieren	Wenn ausgewählt, akzeptiert NTP Nachrichten von einem angegebenen Server oder einem Netzwerk-Broadcast.
NTP-Client-Broadcasts aktivieren	Wenn ausgewählt, akzeptiert NTP Nachrichten nur von Netzwerk-Broadcasts. Diese Methode ist hilfreich, wenn das Netzwerk ausgelastet ist, aber anderen Geräten im Netzwerk vertrauen muss. Wenn diese Option nicht ausgewählt ist, akzeptiert NTP Nachrichten nur von Servern, die in der Liste angegeben sind.
NTP-Server	Zeigt die Netzwerkadresse oder einen Domänennamen eines oder mehrerer NTP-Server an, die das Gerät verwendet. Wenn Sie mehrere Server angeben, prüft das Gerät jede NTP-Nachricht, um die richtige Uhrzeit zu bestimmen.

Kennwort

Verwenden Sie diese Seite, um ein Kennwort für das Gerät anzugeben. Ein sicheres Kennwort besteht aus Buchstaben und Ziffern. Sie können bis zu 15 Zeichen eingeben.

Optionsbeschreibungen

Option	Beschreibung
Benutzer-ID	Diese lautet **scmadmin**. Sie können später weitere Benutzer hinzufügen.
Kennwort	Gibt das neue Kennwort an. Ändern Sie das Kennwort baldmöglichst, damit Ihr Gerät geschützt bleibt. Sie müssen das neue Kennwort zweimal eingeben, um es zu bestätigen. Das ursprüngliche Standardkennwort lautet **scmchangeme**. HINWEIS: Sie müssen das Standardkennwort in ein anderes Kennwort ändern, bevor Sie die Konfiguration anwenden können.

Zusammenfassung

Auf dieser Seite können Sie eine Zusammenfassung der Einstellungen anzeigen, die Sie im Setup-Assistenten vorgenommen haben. Wenn Sie einen Wert ändern möchten, klicken Sie auf den entsprechenden blauen Link, um die Seite anzuzeigen, auf der Sie den Wert ursprünglich eingegeben haben.

Nachdem Sie auf **Fertig stellen** geklickt haben, wird der Setup-Assistent abgeschlossen.

Verwenden Sie die auf dieser Seite angezeigte IP-Adresse, um die Benutzeroberfläche aufzurufen. Beispiel: https://192.168.200.10. Beachten Sie, dass die Adresse mit https und nicht mit http beginnt.

Wenn Sie sich zum ersten Mal bei der Benutzeroberfläche anmelden, geben Sie den Benutzernamen **scmadmin** und das Kennwort ein, das Sie in diesem Setup-Assistenten angegeben haben.

Optionsbeschreibungen

Option	Beschreibung
	Der Wert entspricht bewährten Praktiken.
	Der Wert ist wahrscheinlich nicht korrekt. Er ist zwar gültig, entspricht aber nicht bewährten Praktiken. Prüfen Sie den Wert, bevor Sie fortfahren.
	Es wurde kein Wert festgelegt. Der vorgegebene Standardwert wurde nicht geändert. Prüfen Sie den Wert, bevor Sie fortfahren.

Wiederherstellung aus einer Datei

Wenn Sie Ihren Blade-Server über den Setup-Assistenten innerhalb der Benutzeroberfläche konfigurieren, können Sie mithilfe der Option **Aus Datei wiederherstellen** zuvor gespeicherte Konfigurationsdaten importieren und auf Ihren Blade-Server übernehmen. Nachdem diese Daten importiert wurden, können Sie Änderungen vornehmen, bevor Sie die Konfiguration anwenden.

Option	Beschreibung
Konfigurationsdatei importieren	Gehen Sie zu einer zuvor gespeicherten Konfigurationsdatei, die Sie auf Ihr Gerät hochladen möchten, und wählen Sie diese aus.
Wiederherzustellende Werte	Standardmäßig wird die gesamte Konfiguration wiederhergestellt. Sie können angeben, dass nur bestimmte Teile Ihrer Konfiguration wiederhergestellt werden sollen, indem Sie die Auswahl der übrigen Daten aufheben. Sie erhalten die Gelegenheit zum Überprüfen dieser Änderungen, bevor sie übernommen werden.
Meldungen beim Importieren der Konfiguration	Beim Importieren der Konfigurationsdatei werden Meldungen angezeigt.

Nach dem Importieren der Konfigurationsdaten wird der benutzerdefinierte Modus des **Setup-Assistenten** aktiviert (siehe Durchführen der benutzerdefinierten Einrichtung.) Alle importierten Optionen werden auf den Assistentenseiten angezeigt, sodass Sie die Möglichkeit zum Vornehmen von Änderungen haben, bevor Sie die Konfiguration übernehmen.

▸ Verwenden der Konfigurationskonsole

Erste Schritte mit dem Content Security Blade Server

In diesem Abschnitt erhalten Sie eine Einführung in die Benutzeroberflächenelemente des McAfee Content Security Blade Servers Version 5.6.

Inhalt

- Die Benutzeroberfläche
- Dashboard-Statusinformationen und Konfigurationsoptionen

Die Benutzeroberfläche

Verwenden Sie diese Informationen, um die Elemente der Benutzeroberfläche kennenzulernen.

HINWEIS: Ihre Benutzeroberfläche sieht möglicherweise etwas anders aus als die in Abbildung 11: Das Dashboard gezeigte Oberfläche, da sie in Abhängigkeit von der Anzahl der installierten Blades und der Sprache variieren kann.

Die Benutzeroberfläche enthält die folgenden Elemente:

- **Navigationsleiste**

  Die Navigationsleiste umfasst vier Bereiche: Benutzerinformationen, Abschnittssymbole, Registerkartenleiste und Support-Steuerelemente.

- **Benutzerinformationsleiste**
- **Abschnittssymbole**

  Die Anzahl der Abschnittssymbole hängen von der verwendeten Software-Version ab. Klicken Sie auf ein Symbol, um die Informationen im Inhaltsbereich und in der Registerkartenleiste zu ändern. Die folgenden Symbole sind verfügbar:

Tabelle 2: Abschnittselemente

Symbol	Menü	Funktionen
	Dashboard	Auf dieser Seite finden Sie eine Übersicht über die Appliance. Von hier aus können Sie auf die meisten Seiten zugreifen, die die Appliance steuern.
	Berichte	Auf den Seiten **Berichte** können Sie Ereignisse sehen, die auf der Appliance aufgezeichnet wurden, wie beispielsweise in E-Mails oder beim Web-Zugriff erkannte Viren und Systemaktivitäten wie etwa Details zu kürzlich erfolgten Aktualisierungen und Anmeldungen.

Symbol	Menü	Funktionen
	E-Mail	Mithilfe der Seiten **E-Mail** können Sie Bedrohungen in E-Mails verwalten, infizierte E-Mails isolieren und weitere Aspekte der E-Mail-Konfiguration behandeln.
	Web	Auf den Seiten für das **Web** können Sie Bedrohungen bei Web-Downloads sowie andere Aspekte der Web-Konfiguration verwalten.
	System	Auf den **Systemseiten** können Sie verschiedene Funktionen der Appliance konfigurieren.
	Fehlerbehebung	Auf den Seiten zur **Fehlerbehebung** können Sie sämtliche Probleme im Zusammenhang mit der Appliance analysieren.

- **Registerkartenleiste**

  Die Inhalte der Registerkartenleiste werden durch das ausgewählte Abschnittssymbol bestimmt. Die ausgewählte Registerkarte gibt vor, was im Inhaltsbereich angezeigt wird.

- **Support-Steuerungsschaltflächen**

  Die Support-Steuerungsschaltflächen sind Aktionen, die für den Inhaltsbereich gelten.

  Tabelle 3: Support-Steuerungsschaltflächen

Symbol	Beschreibung
	Aktualisiert den Inhalt.
	Bringt Sie zur zuvor angezeigten Seite zurück. Es wird empfohlen, auf diese Schaltfläche statt auf die Schaltfläche "Zurück" Ihres Browsers zu klicken.
	Dieses Symbol wird angezeigt, wenn Sie etwas konfigurieren, und ermöglicht es Ihnen, Ihre Änderungen anzuwenden.
	Dieses Symbol wird angezeigt, wenn Sie etwas konfigurieren, und ermöglicht es Ihnen, Ihre Änderungen zu verwerfen.
	Öffnet ein Fenster mit Hilfe-Informationen. Viele der Informationen in diesem Fenster finden Sie auch im Produkthandbuch.

- **Steuerelemente anzeigen**

  Die Schaltfläche "Steuerelemente anzeigen" blendet ein Statusfenster ein oder aus.

  Das Statusfenster rechts unten in der Benutzeroberfläche zeigt alle kürzlich erfolgten Aktivitäten an. Neue Meldungen werden oben im Fenster hinzugefügt. Wenn eine Meldung blau und unterstrichen ist, können Sie auf den Link klicken, um eine andere Seite zu besuchen. Sie können das Fenster auch über die Links **Leeren** und **Schließen** verwalten.

- **Inhaltsbereich**

Der Inhaltsbereich enthält den derzeit aktiven Inhalt. Hier findet die meiste Interaktion statt.

HINWEIS: Die vorgenommenen Änderungen werden wirksam, nachdem Sie auf das grüne Häkchen geklickt haben.

Dashboard-Statusinformationen und Konfigurationsoptionen

Das Dashboard bietet eine Zusammenfassung der Aktivitäten der Appliance.

Von dieser Seite aus können Sie auf die meisten Seiten zugreifen, die die Appliance steuern. Auf einer Cluster-Master-Appliance verwenden Sie diese Seite auch, um eine Übersicht der Aktivitäten im Appliance-Cluster anzuzeigen.

HINWEIS: Wenn Sie die Ansicht in einem Bereich ändern möchten, klicken Sie auf **Bearbeiten**, um ein anderes Fenster zu öffnen.

Das Dashboard bietet einen zentralen Ort, an dem Sie Zusammenfassungen der Aktivitäten der Appliance ansehen können.

Abhängig davon, wie Sie Ihre Appliance konfiguriert haben, können Sie Informationen zu Folgendem ansehen:

- Von der Appliance verarbeitete E-Mails
- Gescannter Web-Verkehr
- Gesamtsystemstatus der Appliance
- Aktuelle Erkennungsraten
- Leistung Ihres Netzwerks
- E-Mail-Nachrichten, die von der Appliance in die Warteschlange gestellt wurden
- Anzahl Ihrer eingerichteten Scan-Richtlinien, nach Protokoll getrennt

Sie können auch eine Liste von Links zu Aufgaben konfigurieren, die Sie häufig verwenden. Dies bietet Ihnen eine schnelle und einfache Methode, um zum richtigen Bereich der Benutzeroberfläche zu navigieren.

Im unteren Bereich dieser Seite werden wichtige grafische Informationen zur Leistung der Appliance angezeigt. Jeder dieser Dashboard-Bereiche kann dahingehend angepasst werden, dass er die Informationen anzeigt, die Sie am häufigsten benötigen.

Wenn Sie sich bei der Appliance anmelden und während der Arbeit auf den Konfigurationsseiten der Appliance wird in der unteren rechten Ecke des Bildschirms ein Dialogfeld angezeigt, das Informationen zu empfohlenen Konfigurationsänderungen oder Warnmeldungen hinsichtlich

des Betriebs oder der Einstellungen der Appliance enthält. Sie werden beispielsweise gewarnt, wenn das Global Threat Intelligence-Feedback nicht für alle Richtlinien aktiviert ist.

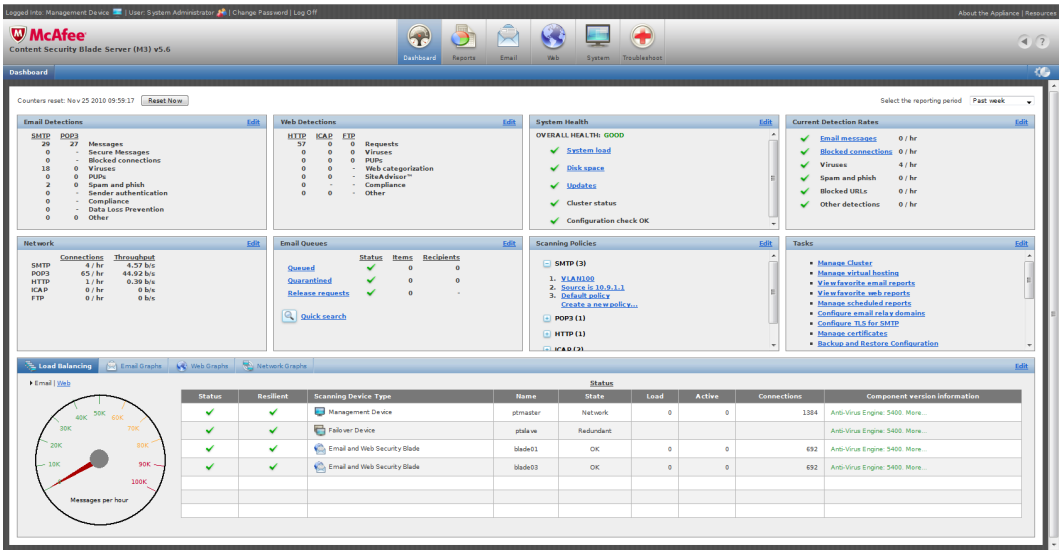


Abbildung 11: Das Dashboard

Bereiche der Seite "Dashboard"

Tabelle 4: Dashboard – Optionsbeschreibungen

Option	Beschreibung
E-Mail-Erkennungen und **Web-Erkennungen**	Zeigt die Anzahl der Erkennungen unter jedem Protokoll an. Klicken Sie auf **Bearbeiten**, um die Ansicht in diesem Fenster zu ändern. Obwohl Sie festlegen können, dass zu einem Protokoll keine Informationen angezeigt werden, scannt die Appliance den Verkehr weiterhin.
Systemstatus	Zeigt den Status wichtiger Komponenten an und ermöglicht Ihnen, Änderungen an den Einstellungen von empfohlenen Systemkonfigurationsänderungen vorzunehmen: • Bei **Aktualisierungen** zeigt ein grünes Häkchen, dass die Komponenten automatisch aktualisiert werden. Wenn Sie eine manuelle Aktualisierung vornehmen möchten, klicken Sie auf den blauen Link. • Für andere Komponenten gibt ein grünes Häkchen an, dass die Komponente innerhalb akzeptabler Grenzwerte betrieben wird. Weiterführende Informationen erhalten Sie, wenn Sie auf die blauen Links klicken. • Sie können die Stufen anpassen, bei denen die Warnhinweissymbole angezeigt werden, und ändern, was im Dialogfeld mit den empfohlenen Konfigurationsänderungen angezeigt wird, indem Sie auf **Bearbeiten** klicken.
Aktuelle Erkennungsraten	Zeigt mithilfe von Symbolen den Status wichtiger Erkennungen der Appliance an.
Netzwerk	Zeigt die Anzahl der Verbindungen unter jedem Protokoll an. Obwohl Sie ein Protokoll nach Klicken auf **Bearbeiten** abwählen können, wickelt die Appliance den Verkehr weiterhin ab.
E-Mail-Warteschlangen	Zeigt mithilfe von Symbolen die Anzahl der Elemente und die Anzahl der Empfänger für jedes Element in den Warteschlangen "In der Warteschlange" und "Anfragen

Option	Beschreibung
	für Entlassen aus Quarantäne" an, die von der Appliance verwaltet werden. Wenn Sie auf die Seiten wechseln möchten, auf denen die Warteschlangen verwaltet werden, klicken Sie auf die blauen Links. Wenn Sie die E-Mails in den Warteschlangen schnell durchsuchen möchten, klicken Sie auf **Schnellsuche**. In der Benutzeroberfläche wird auch angezeigt, wie viele E-Mail-Nachrichten sich in der Warteschlange zum Senden an den McAfee Quarantine Manager befinden und wie viele bereits gesendet wurden.
Scan-Richtlinien	Zeigt eine Liste der von der Appliance eingesetzten Richtlinien an. Obwohl Sie ein Protokoll nach Klicken auf **Bearbeiten** abwählen können, wendet die Appliance weiterhin Richtlinien auf den Verkehr an. Wenn Sie die Scan-Richtlinien anzeigen oder weitere Richtlinien hinzufügen möchten, klicken Sie auf die blauen Links.
Tasks	Zeigt eine Liste häufiger Aufgaben an. Wenn Sie Aufgaben entfernen oder neu organisieren möchten, klicken Sie auf **Bearbeiten**.
Lastenausgleich	Auf einer Master-Cluster-Appliance wird der Status des Appliance-Clusters angezeigt. Um die Einstellungen der Anzeige zu ändern, klicken Sie auf **Bearbeiten**.
Diagramme...	Zeigt Diagramme an, die die zeitliche Aktivität der Appliance darstellen. Obwohl Sie ein Protokoll nach Klicken auf "Bearbeiten" abwählen können, überwacht die Appliance den Verkehr weiterhin.

Lastenausgleich

HINWEIS: Dieser Abschnitt ist nur auf einer Cluster-Master-Appliance oder einem Management-Blade (auf einem Content Security Blade Server) verfügbar.

Tabelle 5: Lastenausgleich – Optionsbeschreibungen

Option	Beschreibung
E-Mail | Web	Wenn Sie hierauf klicken, zeigt die Anzeige Nachrichten pro Stunde (E-Mail) oder Konversationen pro Stunde (Web) an.
Nachrichten pro Stunde (E-Mail) Konversationen pro Stunde (Web)	Zeigt den durchschnittlichen Durchsatz des Clusters auf der Grundlage der alle paar Minuten vorgenommenen Messungen. Wenn ein Cluster doppelt so viele Scan-Appliances umfasst, verdoppelt sich der Durchsatz fast. Zusätzliche Verwaltungsaktivitäten beanspruchen ebenfalls Verarbeitungsleistung.
Status	Zeigt den Status des Geräts an: • – Normaler Betrieb • – Erfordert Aufmerksamkeit • – Erfordert sofortige Aufmerksamkeit
Typ des Scan-Geräts	Zeigt den Typ des Scan-Geräts an: • – Cluster-Master • – Cluster-Failover • – Email and Web Security Appliance

Option	Beschreibung
	• – Email Security Appliance • – Web Security Appliance • – Web Gateway
Name	Zeigt den konfigurierten Namen der Appliance an.
Status	Zeigt den aktuellen Status der einzelnen Appliances an: • **Netzwerk** – Mit dem Netzwerk verbunden. • **Redundant** – Das Cluster-Failover-Gerät arbeitet derzeit nicht, übernimmt jedoch, falls die Master-Cluster-Appliance ausfällt. • **Installieren** – Installieren der Software. • **Synchronisieren** – Synchronisieren mit dem Cluster-Master. • **Starten** – Neustart wird durchgeführt. • **Herunterfahren** – Das Gerät wird heruntergefahren. • **Falsch konfiguriert** – Die Konfigurationsdatei ist fehlerhaft. • **Nicht konfiguriert** – Nicht für den Lastenausgleich konfiguriert. • **Deaktiviert** – Durch den Benutzer deaktiviert. • **Fehlgeschlagen** – Nicht mehr im Netzwerk. Es wurde kein "Heartbeat" erkannt. • **Fehler** – Auf dieser Appliance wurde ein Fehler festgestellt. • **Frühere Version** – Nicht mit dem Lastenausgleich kompatibel.
Auslastung	Zeigt die durchschnittliche Systemauslastung während eines Zeitraums von fünf Minuten an.
Aktiv	Zeigt die Anzahl an aktiven Verbindungen für jede Appliance an. Die Zeile für den Cluster-Master zeigt die Gesamtzahl für alle Appliances an.
Verbindungen	Zeigt die Anzahl an Verbindungen an, die von den einzelnen Appliance verarbeitet wurden, seit die Zähler zum letzten Mal zurückgesetzt wurden.
Informationen zur Komponentenversion	Zeigt die Versionen der Anti-Spam- und Antiviren-DAT-Dateien. Wenn die Appliances auf dem aktuellen Stand sind, stimmen die Versionsnummern überein. Während der Aktualisierung können die Werte voneinander abweichen. Um weitere Informationen anzuzeigen, bewegen Sie den Mauszeiger über den Text, und warten Sie, bis ein gelbes Kästchen angezeigt wird.

Zählerverhalten

Alle Zähler lösen für jede Erkennung einmal aus. Wenn beispielsweise eine Nachricht zwei Anhänge hat, die beide infizierte Inhalte enthalten, wird der **Virenzähler** um zwei erhöht. Die

Informationen in der folgenden Tabelle gelten, sofern nicht anders angegeben, für SMTP- und POP3-Statistiken.

Tabelle 6: Zählerverhalten

Zähler	Verhalten
Nachrichten	Der **SMTP-Zähler** wird in folgenden Fällen um eins erhöht: • Wenn eine TCP-Verbindung zum SMTP-Port auf der Appliance hergestellt wird • Ab dem zweiten <MAIL FROM>-Befehl, wenn mehrere E-Mails in derselben SMTP-Konversation empfangen werden Der **POP3-Zähler** wird für jede Nachricht, die von der Appliance heruntergeladen wird, um eins erhöht.
Sichere Nachrichten	Wird in den folgenden Fällen um eins erhöht: • Wenn ein STARTTLS-Befehl über den Standard-SMTP-Port ausgegeben wird • Wenn die Appliance die TLS-Konversation abfängt, ab dem zweiten <MAIL FROM>-Befehl, wenn mehrere E-Mails in derselben SMTP-Konversation empfangen werden • Wenn Nachrichten über SMTPS gesendet werden
Blockierte Verbindungen	Wird für jedes SYN-Paket um eins erhöht, das von einer IP-Adresse stammt, die eine "Ablehnen, schließen und verweigern (Blockieren)"-Aktion ausgelöst hat. Die RBL-Suchfunktion (Realtime Blackhole List) ist so konfiguriert, dass diese Aktion standardmäßig für die nächsten zehn Minuten ausgeführt wird.
Viren, PUPe, Compliance und Data Loss Prevention	Wird für jede Erkennung um eins erhöht. Wenn beispielsweise eine Nachricht zwei Anhänge hat, die beide infizierte Inhalte enthalten, wird der **Virenzähler** um zwei erhöht.
Spam und Phishing und **Absenderauthentifizierung**	Wird für jede Nachricht, die den Scanner auslöst, um eins erhöht
Sonstige	Wird für jede Erkennung um eins erhöht. Gilt für Nachrichten, die aufgrund ihrer Größe gefiltert werden, Nachrichten, die bei Anti-Relay- und Directory-Harvest-Prüfungen durchfallen, und Nachrichten, die beschädigten Inhalt, geschützten Inhalt, verschlüsselten Inhalt oder signierten Inhalt enthalten.

HINWEIS: Aufgrund der Weise, wie das Dashboard Zähler aggregiert, gibt es eine kleine Differenz zwischen den Informationen, die im Dashboard angezeigt werden, und denen, die in einem geplanten Bericht enthalten sind.

Information zu Statistiken, die in der Liste "E-Mail-Warteschlangen" angezeigt werden

Diese Informationen gelten für die Warteschlangen **In der Warteschlange**, **Isoliert** und **Anfragen für Entlassen aus Quarantäne**:

- Wenn eine Nachricht an zwei Empfänger gesendet und in die Zustellungswarteschlange gestellt wird (beispielsweise, weil der weiterführende MTA ausgefallen ist), gilt Folgendes:
  - Die Anzahl der Elemente in der Warteschlange ist 1, da die Appliance eine Nachricht empfangen hat.

- Die Anzahl der Empfänger ist 2, da die Nachricht zwei Empfänger hat.

  HINWEIS: Wenn Sie auf den Link **In der Warteschlange** klicken, werden zwei Elemente angezeigt, da für jeden Empfänger eine Nachricht vorhanden ist.

- Wenn zwei Nachrichten an einen Empfänger gesendet und in die Zustellungswarteschlange gestellt werden (beispielsweise, weil der weiterführende MTA ausgefallen ist), gilt Folgendes:
  - Die Anzahl der Elemente in der Warteschlange ist 2, da die Appliance zwei Nachrichten empfangen hat.
  - Die Anzahl der Empfänger ist 2, da jede Nachricht einen Empfänger hat.

  HINWEIS: Wenn Sie auf den Link **In der Warteschlange** klicken, werden zwei Elemente angezeigt.

Vorgehensweise – Deaktivieren des Warnhinweises "McAfee Global Threat Intelligence-Feedback deaktiviert"

Die Appliance zeigt standardmäßig eine Warnmeldung an, wenn das McAfee Global Threat Intelligence-Feedback (GTI-Feedback) nicht aktiviert ist, da es von McAfee als bewährte Vorgehensweise angesehen wird, diese Form der Kommunikation zu aktivieren.

1. Wählen Sie im Appliance-Dashboard im Bereich "Systemstatus" die Option **Bearbeiten** aus.
2. Deaktivieren Sie **Einen Warnhinweis anzeigen, wenn McAfee GTI-Feedback nicht aktiviert ist**.
3. Klicken Sie auf **OK**.

Funktionen des Blade-Servers

In diesem Abschnitt erhalten Sie Informationen zu Vorgehensweisen und Szenarien, die die wesentlichen Vorteile beim Einsatz eines Blade-Servers zum Schutz Ihres Gateways aufzeigen.

Zur Durchführung dieser Vorgehensweisen und Szenarien benötigen Sie einige der Informationen, die Sie in der Konfigurationskonsole und im Setup-Assistenten eingegeben haben.

Vorgehensweise

- Demonstrieren der Failover- und Arbeitslastverwaltung
- Testen der Verwaltungsfunktionen auf dem Blade-Server

Demonstrieren der Failover- und Arbeitslastverwaltung

Gehen Sie wie nachfolgend beschrieben vor, um die Arbeitslastverwaltung und die integrierte Redundanzverwaltung des Blade-Servers zu demonstrieren.

Mit dem Blade-Server wird mindestens ein Blade-Server zum Scannen von Inhalten ausgeliefert. Sie können später weitere hinzufügen, falls erforderlich. Für diesen Test wird vorausgesetzt, dass zwei Blades zum Scannen von Inhalten vorhanden sind.

HINWEIS: Informationen zum Hinzufügen und Entfernen von Blades aus dem Gehäuse finden Sie in HP BladeSystem c3000 Enclosure Quick Setup Instructions oder HP BladeSystem c7000 Enclosure Quick Setup Instructions.

Vorgehensweise

1. Wählen Sie auf der Seite **Dashboard | Blade** die Registerkarte **Blade-Status** aus, um sicherzustellen, dass der Blade-Server ordnungsgemäß funktioniert.
   - Der Management-Blade-Server hat den Namen, den Sie mithilfe der Konfigurationskonsole angegeben haben. Der Management-Blade-Server hat den Status **NETZWERK**.
   - Der Failover-Management-Blade-Server hat den Namen, den Sie mithilfe der Konfigurationskonsole angegeben haben. Der Failover-Management-Blade-Server hat den Status **REDUNDANT**.
   - Die Blade-Server zum Scannen von Inhalten werden mit "Blade01", "Blade02" usw. bezeichnet und haben den Status **OK**.
2. Fahren Sie den Management-Blade-Server herunter, nehmen Sie ihn aus dem Gehäuse, und beobachten Sie, wie der Blade-Server unter Einsatz des Failover-Management-Blade-Servers weiterhin funktioniert.
   - Der Status des Failover-Management-Blade-Servers ändert sich in **Netzwerk**.
   - Der Status des Management-Blade-Servers ändert sich in **Fehlgeschlagen**.
3. Wählen Sie unter **System | Cluster-Verwaltung** einen Blade-Server zum Scannen von Inhalten aus, und klicken Sie auf **Deaktivieren**, um diesen Blade-Server zum Scannen von Inhalten zu deaktivieren. Der Blade-Server setzt das Scannen des Datenverkehrs fort.

   VORSICHT: Das Design des Blade-Servers erlaubt die Entfernung eines Blade-Servers zum Scannen von Inhalten aus dem Gehäuse, ohne dass dieser zuerst gestoppt werden muss. McAfee empfiehlt dies jedoch nicht, da ein geringes Risiko besteht, dass dadurch die Informationen auf den Festplattenlaufwerken beschädigt werden könnten.
4. Sehen Sie sich die Spalte **Nachrichten** an, um die Anzahl der Nachrichten zu sehen, die von jedem Blade-Server zum Scannen von Inhalten verarbeitet werden.
5. Wählen Sie unter **Blade-Status** den Blade-Server zum Scannen von Inhalten aus, den Sie deaktiviert haben, und klicken Sie auf **Start**.
6. Sehen Sie sich die Spalte **Nachrichten** erneut an. Der Blade-Server scannt weiteren Datenverkehr und gleicht automatisch die Scan-Last zwischen den beiden Blades aus.
7. *Optional:* Fügen Sie einen dritten Blade-Server zum Scannen von Inhalten zum Gehäuse hinzu, und aktivieren Sie ihn.
8. Sehen Sie sich erneut den **Blade-Status** an. Der Blade-Server scannt noch mehr Nachrichten und gleicht die Scan-Last zwischen den drei Blades aus.

Testen der Verwaltungsfunktionen auf dem Blade-Server

Gehen Sie wie nachfolgend beschrieben vor, um zu demonstrieren, wie die Verwaltungsfunktionen des Blade-Servers Ihren Systemverwaltungsaufwand senken. Das System wird wie ein einziges System verwaltet, unabhängig davon, ob Sie einen oder mehrere Blade-Server zum Scannen von Inhalten einsetzen.

Sie können mithilfe der Status- und Protokolldaten Berichte und Statusinformationen für alle Blades erhalten. Mit dem Management-Blade-Server können Sie DAT-Dateien auf allen Blade-Servern zum Scannen von Inhalten auf dem neuesten Stand halten und darüber hinaus den Quarantäne-Speicherort verwalten.

Blade-Server-Statusinformationen

Während der Datenverkehr den Blade-Server passiert, können Sie das **Dashboard** aufrufen, um aktuelle Informationen zum Gesamtdatendurchsatz, zu Erkennungen und zur Leistung für die einzelnen Protokolle zu erhalten.

Das **Dashboard** enthält die folgenden Blade-spezifischen Informationen:

- **Allgemeiner Status** (Management-Blade-Server und Failover-Management-Blade-Server)
- **Hardware-Status** (Management-Blade-Server)
- **Blade-Status** (alle Blades)

Diese Tabelle zeigt die Informationen an, die Sie zu allen Blades erhalten können.

Geschwindigkeitsmesser	Der durchschnittliche Durchsatz des Blade-Servers auf der Grundlage der alle paar Minuten vorgenommenen Messungen.
Name	Name des Blades: • Der Management-Blade-Server • Der Failover-Management-Blade-Server HINWEIS: Diese Namen werden mithilfe der Konfigurationskonsole angegeben. • Blade <Nummer> – Blade-Server zum Scannen von Inhalten.
Status	Der aktuelle Status der einzelnen Blades.
Auslastung	Die Gesamtsystemauslastung für jedes Blade.
Aktiv	Die Anzahl der derzeit auf jedem Blade aktiven Verbindungen. Die Zeile für den Management-Blade-Server zeigt die Gesamtzahl für alle Blade-Server zum Scannen von Inhalten an.
Verbindungen	Die Gesamtzahl der Verbindungen seit dem letzten Zurücksetzen der Zähler. Die Zeile für den Management-Blade-Server zeigt die Gesamtzahl für alle Blade-Server zum Scannen von Inhalten an.
Weitere Spalten	Versionsinformationen für das Antiviren-Modul, die Antiviren-DAT-Dateien, das Anti-Spam-Modul und die Anti-Spam-Regeln. Wenn die Blades auf dem aktuellen Stand sind, stimmen die Versionsnummern überein. Während der Aktualisierung können die Werte voneinander abweichen.

Generieren von Berichten

Der Content Security Blade Server enthält mehrere vordefinierte Berichte, die Sie im PDF-, HTML- oder Textformat herunterladen können. Sie können den Zeitplan für die Erstellung dieser Berichte definieren und angeben, an wen die Berichte gesendet werden sollen. Sie können auch eigene Berichte erstellen.

Das Blade-Server-Protokoll zeigt Ereignisinformationen für den ausgewählten Berichttyp und den ausgewählten Zeitraum an. Mit den Berichtsfunktionen des Blade-Servers können Sie Berichte erstellen oder Protokolle, Statistiken, Leistungsindikatoren und Diagramme für eine Vielzahl von Daten zum Blade-Server und seinen Aktivitäten anzeigen, beispielsweise die Arbeitsspeicher- und Prozessorauslastung.

Klicken Sie beispielsweise, nachdem Sie die Schritte unter Testen von E-Mail-Verkehr und Virenerkennung ausgeführt haben, auf **E-Mail | Nachrichtensuche**. Die EICAR-Testdatei, die erkannt wurde, wird angezeigt.

Weitere Berichtsinformationen

Sie haben folgende Möglichkeiten:

- Speichern Sie den Bericht unter "Favoriten". Dies ermöglicht Ihnen, denselben Bericht in der Zukunft auszuführen.
- Wechseln Sie, wenn relevant, zwischen verschiedenen Ansichten der Berichtsdaten.

Vorgehensweise

Gehen Sie wie nachfolgend beschrieben vor, um die DAT-Dateien des Blade-Servers zu aktualisieren und anschließend den Aktualisierungsbericht zu lesen.

HINWEIS: Das **Dashboard** wird standardmäßig angezeigt, wenn Sie sich beim Blade-Server anmelden.

1. Wählen Sie **System | Komponentenverwaltung| Aktualisierungsstatus**.
2. Klicken Sie unter **Versionsinformationen und Aktualisierungen** auf **Jetzt aktualisieren** für sämtliche Antiviren- oder Anti-Spam-DAT-Dateiaktualisierungen, die Sie aktualisieren möchten.
3. Wählen Sie **Berichte | Systemberichte**.
4. Wählen Sie **Filter | Updates**.
5. Klicken Sie auf **Übernehmen**. Es werden Informationen zu den Aktualisierungen angezeigt, die auf Ihrem Blade-Server installiert wurden.

Verwenden von Richtlinien für die Verwaltung von Nachrichten-Scans

Gehen Sie wie nachfolgend beschrieben vor, um die Scan-Funktionen des Blade-Servers in Aktion zu erleben. Sie werden detailliert durch das Erstellen und Testen einiger Beispielrichtlinien geführt und erfahren, wie Sie die relevanten Berichte generieren.

Eine Richtlinie ist eine Zusammenstellung von Einstellungen und Regeln, die dem Blade-Server mitteilt, wie er bestimmte Gefahren für Ihr Netzwerk abwehren soll. Wenn Sie Echtzeitscan-Richtlinien für Ihr Unternehmen erstellen, müssen Sie Ihre Anforderungen in Ruhe analysieren und planen. Sie finden Hinweise für die Richtlinienplanung in der *Online-Hilfe*.

Vor dem Erstellen von Richtlinien

Alle Quarantäneaktionen sind standardmäßig deaktiviert. Bevor Sie sie aktivieren, konfigurieren Sie den Blade-Server für die Verwendung von McAfee Quarantine Manager zur Verwaltung des Quarantäne-Speicherorts. Zweck:

1. Wählen Sie in der Benutzeroberfläche **E-Mail | Quarantänekonfiguration**.
2. Wählen Sie **Off-Box-McAfee Quarantine Manager (MQM)-Dienst verwenden**.
3. Geben Sie die Details Ihres McAfee Quarantine Manager ein.

   HINWEIS: Wenn Sie eine vorhandene McAfee-Appliance durch einen McAfee Content Security Blade Server ersetzen, stellen Sie sicher, dass Sie Ihre bestehende **Appliance-ID** verwenden. Mit einer abweichenden **Appliance-ID** ist es nicht möglich, Nachrichten freizugeben, die von der alten Appliance isoliert wurden.

4. Übernehmen Sie Ihre Änderungen.

Erstellen einer Antiviren-Scan-Richtlinie

Eine Antiviren-Scan-Richtlinie soll folgende Aktionen umfassen:

- Viren in eingehenden Nachrichten erkennen
- Die Original-E-Mail isolieren
- Den Empfänger benachrichtigen
- Den Absender warnen

Vorgehensweise

Gehen Sie wie nachfolgend beschrieben vor, um zu zeigen, was passiert, wenn eine Mass-Mailer-Virenregel durch die EICAR-Testdatei ausgelöst wird, und welche Aktionen durchgeführt werden können.

1. Stellen Sie auf dem Gerät sicher, dass Sie McAfee Quarantine Manager verwenden (**E-Mail | Quarantänekonfiguration | Quarantäneoptionen**).
2. Wählen Sie auf dem Gerät **E-Mail | E-Mail-Richtlinien | Scan-Richtlinien**.
   Die Standardrichtlinie wird auf **Säubern oder durch Warnung ersetzen** gesetzt, wenn das Säubern fehlschlägt.
3. Klicken Sie auf **Viren: Säubern oder durch Warnung ersetzen**, um die **Standardeinstellungen für Anti-Virus (SMTP)** anzuzeigen.
4. Stellen Sie unter **Aktionen** im Bereich **Wenn ein Virus erkannt wird** sicher, dass **Säuberung versuchen** ausgewählt ist.
5. Wählen Sie im Abschnitt **Und auch** unter der Aktion die Optionen **Benachrichtigungs-E-Mail an Absender zustellen** und **Isolieren der ursprünglichen E-Mail** aus.
6. Wählen Sie unter **Wenn das Säubern fehlschlägt** die Option **Erkanntes Element durch Warnung ersetzen** aus.
7. Wählen Sie im Abschnitt **Und auch** unter **Wenn das Säubern fehlschlägt** die Optionen **Benachrichtigungs-E-Mail an Absender zustellen** und **Isolieren der ursprünglichen E-Mail** als sekundäre Aktionen aus.
8. Klicken Sie auf **OK**.
9. Wählen Sie **E-Mail | E-Mail-Richtlinien | Scan-Richtlinien [Scanner-Optionen] – Konfiguration der E-Mail-Adresse**.
10. Weisen Sie unter **Gebouncte E-Mails** die E-Mail-Adresse als Administrator-E-Mail-Adresse zu.
    Ohne diese Konfiguration fügt das Gerät keine Absenderadresse zur E-Mail-Benachrichtigung hinzu. Die meisten E-Mail-Server stellen keine E-Mails ohne Absenderadresse zu.
11. Klicken Sie auf **OK** und anschließend auf das grüne Häkchen.
12. Wählen Sie **E-Mail | E-Mail-Richtlinien | Scan-Richtlinien [Antivirus] | Benutzerdefinierte Malware-Optionen**.
13. Wählen Sie **Mass-Mailer**, und setzen Sie anschließend **Bei Erkennung** auf **Verbindung verweigern (Blockieren)**.
    Der Absender-E-Mail-Server empfängt die Fehlermeldung **Code 550: denied by policy** (Durch Richtlinie verweigert). Das Gerät verwaltet eine Liste der Verbindungen, die unter keinen Umständen E-Mails senden dürfen. Die Liste kann unter **E-Mail | E-Mail-Konfiguration | Empfangen von E-Mails | Listen für Zulassen und Verweigern [+] Zugelassene und blockierte Verbindungen** angezeigt werden. Die Option **Verweigerte Verbindungen** ist in der *Online-Hilfe* beschrieben.
14. So testen Sie die Konfiguration:
    a. Senden Sie eine E-Mail von <Client-E-Mail-Adresse> an <Server-E-Mail-Adresse>.

b Erstellen Sie eine Textdatei, die folgende Zeichenfolge enthält:
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

c Speichern Sie die Datei als eicar.txt.

d Hängen Sie die Datei an die E-Mail an.
Das Gateway-Sicherheitsgerät ersetzt die Datei durch eine Warnung, und der Absender wird über den Vorgang benachrichtigt.

15 Kehren Sie zu **Benutzerdefinierte Malware-Optionen** zurück, und klicken Sie auf **Spezifischer Erkennungsname:**.

16 Geben Sie EICAR ein.

17 Stellen Sie sicher, dass als primäre Aktion **Daten zurückweisen und Fehlercode zurückgeben (Blockieren)** festgelegt ist, und klicken Sie anschließend auf **OK**.

18 Erstellen Sie von einem externen E-Mail-Konto aus eine Nachricht, und hängen Sie die EICAR-Testdatei an.
Der E-Mail-Client gibt folgende Fehlermeldung zurück: **Code 550: denied by policy** (Durch Richtlinie verweigert).
E-Mail | E-Mail-Konfiguration | Empfangen von E-Mails | Listen für Zulassen und Ablehnen [+] Blockierte Verbindungen ist leer.

19 Ändern Sie unter **Benutzerdefinierte Malware-Optionen** die primäre Aktion in **Verbindung verweigern**, und klicken Sie anschließend auf **OK**.

20 Senden Sie die E-Mail, und überprüfen Sie die verweigerte Verbindung. Sie weist die IP-Adresse Ihres Client-Computers (Beispiel-IP-Adresse) auf.

21 Senden Sie nun eine reguläre E-Mail. Diese wird aufgrund der Liste der verweigerten Verbindungen ebenfalls abgelehnt. Für den Absender-Server scheint es, als ob der Server nicht online wäre.

Das Gerät prüft die Nachricht, wenn diese auf dem E-Mail-Gateway eingeht, und erkennt, dass sie einen Virus enthält. Die Nachricht wird isoliert, und die vorgesehenen Empfänger und der Absender werden darüber benachrichtigt, dass die Nachricht infiziert war.

Erstellen einer Anti-Spam-Scan-Richtlinie

Gehen Sie wie nachfolgend beschrieben vor, um eine Richtlinie zum Schutz Ihres Unternehmens vor dem Empfang unerwünschter Nachrichten einzurichten.

Eine solche Richtlinie schützt Benutzer vor dem Empfang unerwünschter E-Mail-Nachrichten, die ihre Produktivität senken und den Nachrichtenverkehr über Ihre Server erhöhen.

Vorgehensweise

1 Stellen Sie auf dem Gerät sicher, dass Sie McAfee Quarantine Manager verwenden (E-Mail | Quarantänekonfiguration).

2 Wählen Sie **E-Mail | E-Mail-Richtlinien | Scan-Richtlinien**.
Sie müssen für die SMTP- und POP3-Protokolle jeweils eine separate Anti-Spam-Richtlinie einrichten.

3 Legen Sie die primäre Aktion auf **Daten akzeptieren und verwerfen** fest.

4 Legen Sie die sekundäre Aktion auf **Original-E-Mail isolieren** fest. Ändern Sie den Spam-Faktor auf 5.
Wenn Sie die Spam-Erkennung aktivieren, empfiehlt McAfee, auch die Phishing-Erkennung zu aktivieren. Die Scan-Leistung wird durch das gleichzeitige Ausführen von Anti-Spam- und Anti-Phishing-Tests nicht beeinträchtigt.

5 Erstellen Sie von einem externen E-Mail-Konto aus eine Nachricht, und senden Sie sie an einen Posteingang, der durch das Gerät geschützt wird.

6 Geben Sie folgenden Nachrichtentext ein:
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-E-Mail*C.34X

7 Senden Sie die Nachricht.

8 Öffnen Sie McAfee Quarantine Manager, und sehen Sie sich die Spam-Warteschlange an.

9 Geben Sie die Spam-Nachricht aus der Quarantäne frei.

10 Überprüfen Sie, ob die Nachricht im E-Mail-Konto des Empfängers eingegangen ist.

Erkannte Nachrichten werden an McAfee Quarantine Manager gesendet und können von einem Administrator verwaltet werden.

Erstellen einer Compliance-Richtlinie

Gehen Sie wie nachfolgend beschrieben vor, um eine Richtlinie für die Isolierung eingehender Nachrichten zu erstellen, die unerwünschten Inhalt enthalten. Dies erfolgt nun mithilfe eines Assistenten, der Sie durch den Vorgang führt.

Gehen Sie wie folgt vor, um eine Compliance-Richtlinie einzurichten:

Vorgehensweise

1 Wählen Sie auf dem Gerät **E-Mail | E-Mail-Richtlinien | Wörterbücher**.

2 Wählen Sie **E-Mail-Wörterbuchliste** aus.

3 Zeigen Sie den Bereich **Wörterbuchdetails für ...** an.

4 Wählen Sie **E-Mail | E-Mail-Richtlinien | Scan-Richtlinien**.

5 Wählen Sie unter **Compliance** die Option **Compliance** aus.

6 Wählen Sie **Compliance aktivieren | Ja** aus.

7 Klicken Sie auf **OK**.

8 Klicken Sie unter **Regeln** auf **Neue Regel erstellen**.

9 Geben Sie einen Namen für die Regel ein.

10 Klicken Sie auf **Weiter**.

11 Wählen Sie unter **Einzubeziehende Wörterbücher** die gewünschten Wörterbücher aus. Wählen Sie für diesen Test finanzbezogene Wörterbücher aus.

12 Klicken Sie auf **Weiter**.

13 Wählen Sie unter **Auszuschließende Wörterbücher** die gewünschten Wörterbücher aus.

14 Wählen Sie die durchzuführenden Aktionen aus.

15 Erstellen Sie eine E-Mail auf dem Server von <Beispiel-Server-E-Mail-Adresse> an <Beispiel-Client-E-Mail-Adresse>. Geben Sie folgenden Text ein: Hallo: Wir müssen den bestätigten Wert Ihrer Rente berechnen. Falls sich herausstellt, dass Ihre Anlagen über weniger Kapital verfügen als erwartet, sollten Sie eine Schlichtungsstelle anrufen.

16 Senden Sie die Nachricht.

17 Unter **E-Mail | E-Mail-Zusammenfassung | ZUSAMMENFASSUNG FÜR EINGEHENDE E-MAILS** können Sie die Ergebnisse ansehen.

Der Client-E-Mail-Agent erhält die E-Mail nicht. Das Server-E-Mail-Konto sollte zwei E-Mail-Nachrichten erhalten: eine E-Mail-Benachrichtigung, dass die Nachricht den Compliance-Test nicht bestanden hat, und eine Kopie der ursprünglichen E-Mail.

Informationen zum Verwalten virtueller Hosts

Bei der Verwendung von virtuellen Hosts kann sich ein einzelnes Gerät wie mehrere Geräte verhalten. Jedes *virtuelle* Gerät kann den Datenverkehr innerhalb von angegebenen IP-Adressbereichen verwalten, indem es dem Gerät ermöglicht, Scan-Dienste für den Datenverkehr von vielen Quellen oder Kunden anzubieten.

Vorzüge

- Trennt den Datenverkehr der einzelnen Kunden voneinander.
- Für jeden Kunden oder Host können Richtlinien erstellt werden, was die Konfiguration vereinfacht und Konflikte verhindert, die bei komplexen Richtlinien auftreten können.
- Berichte sind für jeden Kunden oder Host einzeln verfügbar, wodurch die Notwendigkeit einer komplexen Filterung entfällt.
- Falls das Gerät verhaltensbedingt auf eine Reputation-Blacklist gesetzt wird, betrifft dies nur einen virtuellen Host und nicht das gesamte Gerät.

Einrichten der virtuellen Hosts

Die Funktion steht nur für SMTP-Scans zur Verfügung. Den IP-Adressen-Pool für den eingehenden Datenverkehr und den optionalen Adressen-Pool für den ausgehenden Datenverkehr können Sie auf den Seiten **System | Virtuelles Hosting | Virtuelle Hosts** und **System | Virtuelles Hosting | Virtuelle Netzwerke** definieren.

Verwalten der virtuellen Hosts

Funktion	Verhalten
E-Mail-Richtlinie	Jeder virtuelle Host besitzt eine eigene Registerkarte, auf der Sie die Scan-Richtlinien für den Host erstellen können.
E-Mail-Konfiguration	Jeder virtuelle Host besitzt eine eigene Registerkarte, auf der Sie spezielle MTA-Funktionen für den jeweiligen Host konfigurieren können.
E-Mail in der Warteschlange	Sie können alle in der Warteschlange befindlichen E-Mails oder nur die in der Warteschlange befindlichen E-Mails für die einzelnen Hosts anzeigen.
Isolierte E-Mails	Sie können alle isolierten E-Mails oder nur die isolierten E-Mails für die einzelnen Hosts anzeigen.
Berichterstellung	Sie können alle Berichte oder nur die Berichte für die einzelnen Hosts anzeigen.

Verhalten zwischen dem Gerät und MTAs

Wenn das Gerät E-Mails empfängt, die an den IP-Adressbereich des virtuellen Hosts gesendet wurden, führt der virtuelle Host Folgendes aus:

- Er reagiert mit einem eigenen SMTP-Willkommensbanner auf die SMTP-Konversation.
- Er fügt optional seine eigenen Adressinformationen zum Header "Received" hinzu.
- Er scannt die E-Mails gemäß seiner eigenen Richtlinie.

Wenn das Gerät E-Mails zustellt, geschieht Folgendes:

- Die IP-Adresse wird einem Adresspool für ausgehenden Datenverkehr entnommen, oder es wird eine physische IP-Adresse verwendet, wenn kein entsprechender Adresspool angegeben wurde.
- Der empfangende Mailübertragungsagent (MTA) sieht die IP-Adresse des virtuellen Hosts.

- Wenn ein Adresspool vorhanden ist, wird die IP-Adresse nach dem Round-Robin-Verfahren ausgewählt.
- Die EHLO-Antwort wird an den virtuellen Host ausgegeben.

Testen der Konfiguration

Diese Informationen beschreiben, wie Sie testen können, ob der Content Security Blade Server nach der Installation ordnungsgemäß funktioniert. Wenn Sie sich zum ersten Mal bei der Appliance anmelden, wird empfohlen, den Bereich "Systemstatus" des Dashboards zu überprüfen, in dem empfohlene Konfigurationsänderungen angezeigt werden.

Testen der Verbindung

Gehen Sie wie nachfolgend beschrieben vor, um die grundlegende Verbindungsfähigkeit zu bestätigen. Der Blade-Server prüft, ob er mit dem Gateway, den Update-Servern und den DNS-Servern kommunizieren kann. Außerdem wird bestätigt, dass der Name und der Domänenname gültig sind.

Vorgehensweise

1. Öffnen Sie die Seite **Systemtests** mit einer der folgenden Methoden:
   - Wählen Sie im Bereich "Tasks" des Dashboards die Option **Systemtests ausführen**.
   - Wählen Sie in der Navigationsleiste die Option **Fehlerbehebung**.
2. Klicken Sie auf die Registerkarte **Tests**.
3. Klicken Sie auf **Tests starten**. Verifizieren Sie, dass jeder Test positiv ist.

Aktualisieren der DAT-Dateien

Sobald Sie die Konfigurationskonsole ausgefüllt haben, versucht der Content Security Blade Server, alle aktivierten Scanner zu aktualisieren. Gehen Sie wie nachfolgend beschrieben vor, um sicherzustellen, dass Ihr Blade-Server über die aktuellsten Erkennungsdefinitionsdateien (DAT) verfügt.

Im Rahmen der Verwendung des Content Security Blade Servers können Sie einzelne Arten von Definitionsdateien aktualisieren sowie die standardmäßig geplanten Aktualisierungen an Ihre Anforderungen anpassen.

Vorgehensweise

1. Öffnen Sie die Seite **Aktualisierungen** mit einer der folgenden Methoden:
   - Wählen Sie im Bereich **Systemstatus** des Dashboards die Option **Aktualisierungen**.
   - Wählen Sie **System | Komponentenverwaltung| Aktualisierungsstatus**.
2. Wenn Sie alle DAT-Dateien aktualisieren möchten, klicken Sie neben der Antiviren-Modul-Komponente auf **Jetzt aktualisieren**.

Testen von E-Mail-Verkehr und Virenerkennung

Gehen Sie wie nachfolgend beschrieben vor, um zu überprüfen, ob E-Mail-Verkehr erfolgreich durch Ihren Blade-Server geleitet wird und ob Bedrohungen ordnungsgemäß identifiziert werden. McAfee verwendet die EICAR-Testdatei, eine harmlose Datei, die eine Virenerkennung auslöst.

Vorgehensweise

1. Senden Sie eine E-Mail von einem externen E-Mail-Konto (wie Hotmail) an einen internen Posteingang, und vergewissern Sie sich, dass die E-Mail angekommen ist.
2. Sehen Sie sich im Dashboard den Bereich **E-Mail-Erkennungen** an. Aus der Liste für das Protokoll, das Sie zum Versenden der Nachricht verwendet haben, sollte hervorgehen, dass eine Nachricht empfangen wurde.
3. Kopieren Sie die folgende Zeile in eine Datei, und achten Sie dabei darauf, dass Sie keine Leerzeichen oder Zeilenumbrüche hinzufügen:

   X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARDANTIVIRUS-TEST-FILE!$H+H*
4. Speichern Sie die Datei unter dem Namen EICAR.COM.
5. Erstellen Sie von einem externen E-Mail-Konto (SMTP-Client) aus eine Nachricht mit der Datei EICAR.COM als Anhang, und senden Sie die Nachricht an einen internen Posteingang.
6. Kehren Sie zum Dashboard zurück, und sehen Sie sich den Bereich **E-Mail-Erkennungen** an. Sie sollten sehen, dass ein Virus erkannt wurde.
7. Löschen Sie die Nachricht, wenn Sie das Testen Ihrer Installation abgeschlossen haben, damit ahnungslose Benutzer keinen Schreck bekommen.

Testen der Spam-Erkennung

Gehen Sie wie nachfolgend beschrieben vor, um einen "General Test mail for Unsolicited Bulk Email" (Allgemeinen Test auf unerwünschte Bulk-E-Mails – GTUBE) auszuführen, mit dem geprüft wird, ob eingehender Spam erkannt wird.

Vorgehensweise

1. Erstellen Sie von einem externen E-Mail-Konto (SMTP-Client) aus eine neue E-Mail.
2. Kopieren Sie den folgenden Text in den Nachrichtenteil der E-Mail:

   XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARDANTI-UBE-TEST-EMAIL*C.34X

   Vergewissern Sie sich, dass Sie keine Leerzeichen oder Zeilenumbrüche eingeben.
3. Senden Sie die neue E-Mail an eine interne Posteingangsadresse. Die Software scannt die Nachricht, erkennt sie als Junk-E-Mail und verarbeitet sie entsprechend. Der GTUBE-Test hat Vorrang vor Blacklists und Whitelists.

Testen von Web-Verkehr und Virenerkennung

Gehen Sie folgendermaßen vor, um zu prüfen, ob Web-Verkehr erfolgreich durch den Content Security Blade Server geleitet wird.

Vorgehensweise

1. Rufen Sie eine externe Website auf, damit eine öffentliche Verbindung genutzt wird.

2 Gehen Sie zum Dashboard. Aus der HTTP-Liste geht hervor, dass Sie eine Website aufgerufen haben.

3 Rufen Sie die EICAR-Website (http://www.eicar.org) auf, und öffnen Sie die EICAR-Testdatei.

4 Kehren Sie zum Dashboard zurück, und sehen Sie sich den Bereich **Web-Erkennungen** an. Aus der HTTP-Liste geht hervor, dass ein Virus erkannt wurde.

Funktionen des Content Security Blade Servers

In diesem Abschnitt finden Sie Vorgehensweisen zur Demonstration der Scan-Funktionen des Content Security Blade Servers. Sie werden detailliert durch das Erstellen und Testen einiger Beispielrichtlinien geführt und erfahren, wie Sie die relevanten Berichte generieren.

Inhalt

- Vermeiden des Verlusts vertraulicher Daten
- Bearbeiten von isolierten Nachrichten

Scan-Richtlinien und deren Einfluss auf Ihr Netzwerk

Eine Richtlinie ist eine Zusammenstellung von Einstellungen und Regeln, die dem Content Security Blade Server mitteilt, wie er bestimmte Gefahren für Ihr Netzwerk abwehren soll. Wenn Sie Echtzeitscan-Richtlinien für Ihr Unternehmen erstellen, müssen Sie Ihre Anforderungen in Ruhe analysieren und planen. Hinweise für die Richtlinienplanung finden Sie in der Online-Hilfe, die über die Produktbenutzeroberfläche aufgerufen werden kann.

Inhaltsscans unter Verwendung der E-Mail-Compliance-Regeln

Verwenden Sie Compliance-Scans zur Unterstützung der Compliance mit gesetzlichen und betrieblichen Auflagen. Sie können aus einer Bibliothek aus vordefinierten Compliance-Regeln wählen oder eigene Regeln und Wörterbücher für Ihr Unternehmen erstellen.

Compliance-Regeln können hinsichtlich ihrer Komplexität von einem einfachen Auslöser bei der Erkennung eines einzelnen Begriffs in einem Wörterbuch bis hin zum Aufbauen auf und Kombinieren von faktorbasierten Wörterbüchern variieren, die nur auslösen, wenn ein bestimmter Schwellenwert erreicht wird. Mithilfe der erweiterten Funktionen von Compliance-Regeln können Wörterbücher mit den logischen Operationen "eines von", "alle von" oder "außer" kombiniert werden.

1 Gehen Sie wie folgt vor, um E-Mail-Nachrichten zu blockieren, die die Richtlinie "Bedrohliche Sprache" verletzen:

   a Navigieren Sie zu **E-Mail | E-Mail-Richtlinien | Scan-Richtlinien**, und wählen Sie **Compliance**.

   b Klicken Sie im Dialogfeld **Standard-Compliance-Einstellungen** auf **Ja**, um die Richtlinie zu aktivieren.

   c Klicken Sie auf **Neue Regel aus Vorlage erstellen**, um den Assistenten für die Regelerstellung zu öffnen.

   d Wählen Sie die Richtlinie **Zulässige Nutzung - Bedrohliche Sprache** aus, und klicken Sie auf **Weiter**.

   e Sie können den Namen der Regel optional ändern. Klicken Sie anschließend auf **Weiter**.

f Ändern Sie die primäre Aktion in **Daten akzeptieren und anschließend verwerfen (Blockieren)**, und klicken Sie auf **Fertig stellen**.

g Klicken Sie auf **OK**, und übernehmen Sie die Änderungen.

2 Gehen Sie wie folgt vor, um eine einfache benutzerdefinierte Regel zum Blockieren von E-Mail-Nachrichten zu erstellen, die Sozialversicherungsnummern enthalten:

a Navigieren Sie zu **E-Mail | E-Mail-Richtlinien | Scan-Richtlinien**, und wählen Sie **Compliance**.

b Klicken Sie im Dialogfeld **Standard-Compliance-Einstellungen** auf **Ja**, um die Richtlinie zu aktivieren.

c Klicken Sie auf **Neue Regel erstellen**, um den **Assistenten für die Regelerstellung** zu öffnen.

d Geben Sie einen Namen für die Regel ein, und klicken Sie auf **Weiter**.

e Geben Sie im **Suchfeld** sozial ein.

f Wählen Sie das Wörterbuch **Sozialversicherungsnummer** aus, und klicken Sie zweimal auf **Weiter**.

g Wählen Sie die Aktion **Daten akzeptieren und anschließend verwerfen (Blockieren)**, und klicken Sie auf **Fertig stellen**.

3 Gehen Sie wie folgt vor, um eine komplexe Regel zu erstellen, die auslöst, wenn sowohl Wörterbuch A als auch Wörterbuch B erkannt werden, jedoch nicht, wenn darüber hinaus auch Wörterbuch C erkannt wird:

a Navigieren Sie zu **E-Mail | E-Mail-Richtlinien | Scan-Richtlinien**, und wählen Sie **Compliance**.

b Klicken Sie im Dialogfeld **Standard-Compliance-Einstellungen** auf **Ja**, um die Richtlinie zu aktivieren.

c Klicken Sie auf **Neue Regel erstellen**, um den Assistenten für die Regelerstellung zu öffnen.

d Geben Sie einen Namen für die Regel ein, und klicken Sie auf **Weiter**.

e Wählen Sie zwei Wörterbücher aus, die in die Regel aufgenommen werden sollen, und klicken Sie auf **Weiter**.

f Wählen Sie in der Ausschlussliste ein Wörterbuch aus, das Sie von der Regel ausschließen möchten.

g Wählen Sie die Aktion aus, die ausgeführt werden soll, wenn die Regel ausgelöst wird.

h Wählen Sie im Dropdown-Feld **Und bedingt** die Option **Alle** aus, und klicken Sie auf **Fertig stellen**.

4 Gehen Sie wie folgt vor, um ein neues Wörterbuch zu einer vorhandenen Regel hinzuzufügen:

a Navigieren Sie zu **E-Mail | E-Mail-Richtlinien | Scan-Richtlinien**, und wählen Sie **Compliance**.

b Erweitern Sie die Regel, die Sie bearbeiten möchten.

c Wählen Sie **Wörterbuch hinzufügen**.

d Wählen Sie das neue Wörterbuch aus, das Sie hinzufügen möchten, und klicken Sie auf **OK**.

5 Gehen Sie wie folgt vor, um eine "Unzufriedenheit"-Regel zu konfigurieren, die mit einem niedrigen Schwellenwert überwacht wird und bei einem hohen Schwellenwert blockiert:

a Navigieren Sie zu **E-Mail | E-Mail-Richtlinien | Scan-Richtlinien**, und wählen Sie **Compliance**.

b Klicken Sie auf **Neue Regel erstellen**, geben Sie einen Namen für die Regel ein, beispielsweise Unzufriedenheit - Niedrig, und klicken Sie auf **Weiter**.

c Wählen Sie das Wörterbuch "Unzufriedenheit" aus, und geben Sie unter "Schwelle" den Wert 20 ein.

d Klicken Sie auf **Weiter** und anschließend erneut auf **Weiter**.

e Akzeptieren Sie unter **Wenn die Compliance-Regel ausgelöst wird** die Standardaktion.

f Klicken Sie auf **Fertig stellen**.

g Wiederholen Sie die Schritte 2 bis 4, um eine weitere neue Regel zu erstellen. Nennen Sie diese jedoch Unzufriedenheit – Hoch, und weisen Sie ihr den Schwellenwert 40 zu.

h Wählen Sie unter **Wenn die Compliance-Regel ausgelöst wird** die Option **Daten akzeptieren und anschließend verwerfen (Blockieren)** aus.

i Klicken Sie auf **Fertig stellen**.

j Klicken Sie auf **OK**, und übernehmen Sie die Änderungen.

6 Gehen Sie wie folgt vor, um den Schwellenwert zu bearbeiten, der einer vorhandenen Regel zugeordnet ist. Bei dieser Vorgehensweise wird davon ausgegangen, dass Ihre Regel ein Wörterbuch enthält, das die Aktion basierend auf einem Schwellenwert auslöst, beispielsweise das Wörterbuch "Vergütung und Leistungen":

a Navigieren Sie zu **E-Mail | E-Mail-Richtlinien | Scan-Richtlinien**, und wählen Sie **Compliance**.

b Erweitern Sie die Regel, die Sie bearbeiten möchten, und wählen Sie anschließend das Symbol "Bearbeiten" neben dem Wörterbuch aus, dessen Faktor Sie ändern möchten.

c Geben Sie unter "Schwellenwert für Wörterbuch" den Faktor ein, bei dem die Regel ausgelöst werden soll, und klicken Sie auf **OK**.

7 Gehen Sie wie folgt vor, um den Faktorbeitrag eines Wörterbuchbegriffs zu beschränken. Bei dieser Vorgehensweise wird davon ausgegangen, dass Ihre Regel ein Wörterbuch enthält, das die Aktion basierend auf einem Schwellenwert auslöst, beispielsweise das Wörterbuch "Vergütung und Leistungen". Bei solchen Wörterbüchern können Sie beschränken, wie oft ein Begriff zum Gesamtfaktor beitragen kann.

a Navigieren Sie zu **E-Mail | E-Mail-Richtlinien | Scan-Richtlinien**, und wählen Sie **Compliance**.

b Erweitern Sie die Regel, die Sie bearbeiten möchten, und klicken Sie anschließend auf das Symbol "Bearbeiten" neben dem Wörterbuch, dessen Faktor Sie ändern möchten.

c Geben Sie unter **Max. Begriffsanzahl** die maximale Anzahl an Vorkommnissen eines Begriffs an, die zum Gesamtfaktor beitragen sollen.

HINWEIS: Sie können dieselbe Richtlinie auf Web-Mail anwenden, indem Sie die HTTP-Richtlinie bearbeiten.

Vermeiden des Verlusts vertraulicher Daten

Gehen Sie wie nachfolgend beschrieben vor, um das Versenden eines vertraulichen Finanzdokuments aus Ihrem Unternehmen heraus zu blockieren.

Vorgehensweise

1. Navigieren Sie zu **E-Mail | E-Mail-Richtlinien | Registrierte Dokumente**, und erstellen Sie die Kategorie Finanzen.
2. Navigieren Sie zu **E-Mail | E-Mail-Richtlinien | Scan-Richtlinie**, und wählen Sie die **Data Loss Prevention**-Richtlinie aus.
3. Klicken Sie im Dialogfeld **Standardeinstellungen für Data Loss Prevention** auf **Ja**, um die Richtlinie zu aktivieren.
4. Klicken Sie auf **Neue Regel erstellen**, wählen Sie die Kategorie "Finanzen" aus, und klicken Sie auf **OK**, damit die Kategorie in der Liste "Regeln" angezeigt wird.
5. Wählen Sie die der Kategorie zugeordnete Aktion aus, ändern Sie die primäre Aktion in **Daten akzeptieren und anschließend verwerfen (Blockieren)**, und klicken Sie auf **OK**.
6. Klicken Sie erneut auf **OK**, und übernehmen Sie die Änderungen.

Bearbeiten von isolierten Nachrichten

Der McAfee® Content Security Blade Server verwendet die Software McAfee® Quarantine Manager und stellt damit eine Off-Box-Quarantänelösung für Ihre E-Mail-Nachrichten bereit.

Nähere Informationen dazu, wo Sie die isolierten Nachrichten finden, entnehmen Sie bitte Dokumentation zu McAfee® Quarantine Manager.

Überwachen der Spam-Erkennung

Gehen Sie wie nachfolgend beschrieben vor, um die Spam-Erkennungsrate mit der standardmäßigen SMTP-Spam-Erkennungsrichtlinie überwachen. Sobald Sie die Konfigurationskonsole ausgeführt haben, funktionieren diese Einstellungen und schützen Ihr Netzwerk und Ihre Benutzer vor unerwünschten Spam-Nachrichten. Eine ausführlichere Erläuterung der Einstellungen finden Sie in der Online-Hilfe, die über die Benutzeroberfläche aufgerufen werden kann.

Standardmäßig gilt für den Content Security Blade Server Folgendes:

- Phishing-Nachrichten werden blockiert.
- Nachrichten mit einer Einstufung von mindestens fünf werden als Spam markiert.
- Spam-Nachrichten mit einer Einstufung von mindestens zehn werden verworfen.
- Die Absenderauthentifizierung ist aktiviert.

Mithilfe dieser Standardeinstellungen erkennt der Content Security Blade Server mehr als 98 % aller Spam-Nachrichten.

HINWEIS: Die Einstellungen für die Absenderauthentifizierung umfassen die E-Mail-Reputation von McAfee Global Threat Intelligence. Wenn ein Absender die E-Mail-Reputation-Prüfung von McAfee Global Threat Intelligence nicht besteht, weist die Blade-Server die E-Mail zurück, beendet die Verbindung und lässt die IP-Adresse des Absenders nicht mehr zu. Die IP-Adresse des Absenders wird zu einer Liste blockierter Verbindungen hinzugefügt und automatisch zehn Minuten lang auf Kernel-Ebene blockiert (die standardmäßige Blockierdauer kann geändert werden). Im Bereich **E-Mail-Erkennungen** des Dashboards wird die Anzahl der blockierten Verbindungen angezeigt.

Vorgehensweise

1. Wählen Sie im Bereich **Scan-Richtlinien** des Dashboards die Option **SMTP | Standardrichtlinie**, um die Standardeinstellungen für die Spam-Erkennung anzuzeigen.
2. Vergewissern Sie sich, dass Spam-Nachrichten ordnungsgemäß identifiziert werden, indem Sie eine Nachricht den Content Security Blade Server passieren lassen, bei der die Einstellungen zur Spam-Erkennung aktiviert werden.
3. Wenn Sie die Erkennungsrate überwachen möchten, kehren Sie zum Dashboard zurück, und betrachten Sie den Bereich **E-Mail-Erkennungen**.
   Die Zahl für **Spam und Phishing** und für **Absenderauthentifizierung** wird hochgezählt. Die Zahl für die Absenderauthentifizierungserkennungen beinhaltet die Anzahl der Absender, die die E-Mail-Reputation-Prüfung von McAfee Global Threat Intelligence nicht bestanden haben. **E-Mail-Diagramme** bietet eine graphische Darstellung der Daten.
4. Wenn Sie einen Bericht über die E-Mail-Aktivität erhalten möchten, gehen Sie zu **Tasks**, und wählen Sie **Bevorzugte E-Mail-Berichte anzeigen**.
5. Sehen Sie sich den Bericht **Blockiert (heute)** und den Bericht **Häufigste Spam-Absender (heute)** an.

Überwachen der Web-Aktivität

Gehen Sie wie nachfolgend beschrieben vor, um zu sehen, wie SiteAdvisor und die Standardeinstellungen für die Web-Kategorisierung bei HTTP aktiv sind. Sobald Sie den Setup-Vorgang abgeschlossen haben, funktionieren diese Einstellungen und schützen Ihr Netzwerk und Ihre Benutzer vor gefährlichen oder schädlichen Websites.

Vorgehensweise

1. Wählen Sie im Bereich **Scan-Richtlinien** des Dashboards die Option **HTTP**, und klicken Sie auf **Standardrichtlinie**.
2. Wählen Sie **McAfee GTI-Web-Reputation und Kategorisierung**, um die Standardeinstellungen anzuzeigen. SiteAdvisor verwehrt den Zugriff auf einen URL, wenn die Site mit der Klassifizierung **Warnung** beurteilt wird.
3. Wenn Sie überprüfen möchten, ob SiteAdvisor HTTP-Verkehr ordnungsgemäß scannt, rufen Sie folgende Adresse auf: http://warn.siteadvisor.
4. Kehren Sie zum Dashboard zurück, und sehen Sie sich den Bereich **Web-Erkennungen** an. In der Spalte "HTTP" wird der SiteAdvisor-Eintrag hochgezählt.
5. Wenn Sie eine visuelle Darstellung der Web-Reputation-Aktivität vom Dashboard aus sehen möchten, gibt es hierfür unter **Web-Diagramme** eine SiteAdvisor-Leiste.
6. Klicken Sie im Bereich **Tasks** auf **Bevorzugte Web-Berichte anzeigen**, und wählen Sie **Web-Berichte**.
7. Aus dem Bericht **Blockiert (SiteAdvisor, letzte 24 Stunden)** geht hervor, wie viele Web-Anfragen an dem betreffenden Tag blockiert, geändert oder überwacht wurden.
8. Aus dem Bericht **Liste häufigster URLs** sind die an dem betreffenden Tag am häufigsten geöffneten URLs ersichtlich.

Betrieb im ausfallsicheren Modus

Mit der Version 5.6 des McAfee® Content Security Blade Server wird für den Blade-Server ein ausfallsicherer Betriebsmodus eingeführt. In diesem Modus werden alle Verbindungen zwischen Ihrem Netzwerk und dem Blade-Server sowie die Verbindungen innerhalb des Blade-Server-Gehäuses so ausgelegt, dass mehrere Pfade verwendet werden können.

Auf diese Weise kann der Ausfall von Serverkomponenten, Netzwerkgeräten oder Verkabelung, die für Weiterleitung des Datenverkehrs zwischen Ihrem Netzwerk und dem Blade-Server verwendet werden, besser verkraftet werden.

Inhalt

- Nutzung der Hardware im ausfallsicheren Modus
- Entscheidung treffen zur Verwendung des ausfallsicheren Modus
- Vor dem Umkonfigurieren in den ausfallsicheren Modus
- Aktivieren des ausfallsicheren Modus

Nutzung der Hardware im ausfallsicheren Modus

Im ausfallsicheren Modus werden die Netzwerkverbindungen in folgende Segmente innerhalb und außerhalb des Blade-Server-Gehäuses aufgeteilt:

- LAN1 und LAN2 werden für Verbindungen mit externen Netzwerken zur Übertragung des gescannten Datenverkehrs genutzt. Diese werden entweder für getrennte Netzwerke (in den Modi "Expliziter Proxy" oder "Transparenter Router") oder für die beiden Anschlüsse im Modus "Transparente Bridge" verwendet.

  Der gescannte Datenverkehr wird immer über alle aktiven Interconnect-Module übertragen, um einen maximalen Durchsatz und maximale Ausfallsicherheit zu gewährleisten.

- Das Out-of-Band-Netzwerk (OOB) ermöglicht es, den Datenverkehr für die Verwaltung vom gescannten Datenverkehr getrennt zu halten. Wenn es eingesetzt wird, kann das System so konfiguriert werden, dass keine Verwaltungsarbeiten über die LAN1- und LAN2-Netzwerke erfolgen können.

  Im M7-Gehäuse wird das OOB-Netzwerk normalerweise über zwei direkte Passthrough-Module bereitgestellt, was eine aktive/passive Redundanz ermöglicht.

  Im M3-Gehäuse wird das OOB-Netzwerk über das LAN2-Interconnect-Modul auf einem getrennten VLAN mit getrennten Switch-Verbindungen übertragen.

  HINWEIS: Mit beiden Gehäusen ist es möglich, das OOB-Netzwerk alternativ über ein VLAN-Netzwerk auf denselben externen Anschlüssen der Interconnect-Module LAN1 und LAN2 zu übertragen.

- Der Datenverkehr zwischen den Management-Blade-Servern und den Scan-Blades wird auf einem separaten VLAN innerhalb des Blade-Server-Gehäuses abgewickelt. Dabei handelt es

sich um ein privates VLAN innerhalb des Gehäuses, das normalerweise außerhalb des Gehäuses nicht zur Verfügung steht.

Das Scanning-VLAN ist auf den Management-Blade-Servern gekennzeichnet, auf den Scan-Blades jedoch nicht gekennzeichnet. Dadurch funktioniert die PXE-Installation (Preboot Execution Environment) der Scan-Blades wie erwartet.

HINWEIS: Die Konfiguration der Interconnect-Module ist für Management-Blade-Server und Scan-Blades unterschiedlich. McAfee empfiehlt, dass Sie nur die in diesem Dokument empfohlenen Blade-Steckplätze für die Management- und Scan-Blades verwenden, um Konfigurationsprobleme zu vermeiden.

Im Gehäuse werden vier Interconnect-Module verwendet, um eine Ausfallsicherheit im Falle des Ausfalls einer der oben beschriebenen Netzwerkverbindungen zu gewährleisten. Die Ausfallsicherheit ist bei folgenden Ausfällen gegeben:

- Ausfall einer externen Verbindung

  Die Ausfallsicherheit bei externen Verbindungen wird durch die Unterstützung von aggregierten Verbindungen (auch als Bonding, Trunking, Port Channel oder Etherchannel bezeichnet) ermöglicht. Es können bis zu fünf Verbindungen gebündelt werden, um eine maximale Ausfallsicherheit zu erreichen. Vom Ausfall einer einzelnen Verbindung sind nur die Pakete betroffen, die zum Zeitpunkt des Ausfalls über die jeweilige Verbindung übertragen werden. Das Interconnect-Modul und die benachbarte Infrastruktur stoppen automatisch die Nutzung der ausgefallenen Verbindung.

- Ausfall einer internen Verbindung

  Intern werden Querverbindungspaare verwendet, um eine redundante Konnektivität zwischen benachbarten Interconnect-Modulen zu gewährleisten. Dies bedeutet, dass beim Ausfall aller Verbindungen im Blade-Gehäuse, die extern zum Interconnect-Modul sind, der Datenverkehr weiterhin über das benachbarte Interconnect-Modul und über die Querverbindung zum Original-Blade erfolgen kann. Vom Ausfall einer Verbindung sind nur die Pakete betroffen, die zum Zeitpunkt des Ausfalls über die jeweilige Verbindung übertragen werden. STP wird zur Vermeidung von Netzwerk-Loops verwendet.

- Ausfall einer Blade-Netzwerkkarte

  Alle Blades verfügen über zwei Pfade zu jedem Netzwerk. Wenn eine Netzwerkkarte (oder deren Anschluss an das Interconnect-Modul) ausfällt, gibt es immer einen redundanten Pfad zum Switch-Netzwerk. Vom Ausfall einer Netzwerkkarte sind nur die Pakete betroffen, die zum Zeitpunkt des Ausfalls über die jeweilige Verbindung übertragen werden.

- Ausfall eines Scan-Blades

  Bei Ausfall eines Scan-Blades leitet der Management-Blade-Server den Scan-Datenverkehr automatisch an die verbleibenden Scan-Blades. Verbindungen zum Zeitpunkt des Ausfalls werden unterbrochen.

- Ausfall eines Management-Blade-Servers

  Bei Ausfall eines Management-Blade-Servers wird der Failover-Blade zum Master und setzt die Verteilung des Datenverkehrs an die Scan-Blades fort. Verbindungen zum Zeitpunkt des Ausfalls werden unterbrochen.

- Ausfall eines Interconnect-Moduls

  Dies wird ähnlich wie der Ausfall von internen und externen Verbindungen gehandhabt. Der gesamte Datenverkehr wird an und über das verbleibende Interconnect-Modul geleitet.

▸ Betrieb im ausfallsicheren Modus

Entscheidung treffen zur Verwendung des ausfallsicheren Modus

Im Standardmodus (nicht ausfallsicher) verwendet der McAfee Content Security Blade Server ein Interconnect-Modul für jedes LAN (LAN1 und LAN2), das für Ihren Blade-Server erforderlich ist.

Im ausfallsicheren Modus werden für jedes LAN zwei Interconnect-Module verwendet, sodass für LAN1 und LAN2 jeweils mehrere Netzwerkpfade aufgebaut werden können.

HINWEIS: Den Blade-Server für den ausfallsicheren Modus einzurichten ist wesentlich komplexer als die Einrichtung des Standardmodus. Daher empfiehlt McAfee, den ausfallsicheren Modus nur dann zu verwenden, wenn Sie in der Lage sind, die erforderlichen Änderungen am Netzwerk und an anderen Komponenten vorzunehmen.

Falls Sie planen, auf Ihrem McAfee® Content Security Blade Server der Version 5.6 den ausfallsicheren Modus zu verwenden, empfiehlt McAfee, Ihren Blade-Server zunächst im Standardmodus (nicht ausfallsicher) zu installieren, um sicherzustellen, dass der Blade-Server wie erwartet funktioniert.

Wenn alle Komponenten ordnungsgemäß arbeiten, konfigurieren Sie Ihren Blade-Server für den Betrieb im ausfallsicheren Modus um. In den folgenden Abschnitten werden die Schritte detailliert beschrieben, die für die Konfiguration Ihres Blade-Servers im Standardmodus (nicht ausfallsicher) notwendig sind. Im Anschluss wird erläutert, wie die notwendigen Änderungen für die Verwendung des ausfallsicheren Modus vorzunehmen sind, falls gewünscht.

- Betrieb im ausfallsicheren Modus

Vor dem Umkonfigurieren in den ausfallsicheren Modus

McAfee empfiehlt, dass Sie sich Zugriff auf die unter Planen der Installation aufgeführten Informationen beschaffen, bevor Sie damit beginnen, Ihren McAfee® Content Security Blade Server für den Betrieb im ausfallsicheren Modus umzukonfigurieren.

- Betrieb im ausfallsicheren Modus
- Hardware-Informationen
- Benutzernamen und Kennwörter

Hardware-Informationen

Damit Ihre Hardware im ausfallsicheren Modus betrieben werden kann, muss Folgendes verfügbar sein:

- Eine Mindestanzahl an Blades.

  Für den ausfallsicheren Modus wird mindestens benötigt:

  - Ein Management-Blade-Server
  - Ein Failover-Management-Blade-Server
  - Mindestens zwei Scan-Blades
- Eine ausreichende Anzahl von Netzwerkkarten in allen Blades

Wenn Sie einen neuen McAfee® Content Security Blade Server installieren, ist die gelieferte Hardware für den ausfallsicheren Modus geeignet.

Wenn Sie jedoch einen bereits installierten McAfee® Content Security Blade Server für den Betrieb im ausfallsicheren Modus umkonfigurieren, müssen Sie möglicherweise ein Upgrade der einzelnen Blades durchführen und Tochterkarten in den Blades installieren. Die Management- und Failover-Management-Blade-Server müssen in beiden Steckplätzen mit Tochterkarten gemäß McAfee-Spezifikationen ausgerüstet sein.

Wenn Sie einen Content Security Blade Server mit M3-Gehäuse verwenden, benötigen alle Scan-Blades mindestens eine Tochterkarte im Fach 1.

Sie können in der Benutzeroberfläche des Onboard Administrator prüfen, ob diese Karten vorhanden sind. Prüfen Sie, ob Tochterkarten im Register **Information** der Anzeige **Device Bay** (Gerätefach) aufgeführt sind.

HINWEIS: Die Tochterkarten müssen vom richtigen Typ sein und sich in den richtigen Steckplätzen befinden. Dual-Port-Tochterkarten müssen im Fach 1 installiert sein, Quad-Port-Karten im Fach 2.

- Der Management-Blade-Server befindet sich im Blade-Fach 1 des Gehäuses.
- Der Failover-Management-Blade-Server befindet sich im Blade-Fach 2 des Gehäuses.
- Die Software Email and Web Security 5.6 steht zur Installation entweder auf einer CD-ROM, einem USB-Stick oder über den Onboard Administrator zur Verfügung.
- Interconnect-Module.
  - Interconnect-Module des Typs HP GBe2c müssen in den Interconnect-Modul-Fächern 1 bis 4 installiert sein.

    Beim Content Security Blade Server im M7-Gehäuse müssen Passthrough-Module in den Interconnect-Modul-Fächern 5 und 6 installiert sein, um die OOB-Konnektivität zu ermöglichen.
- Module für den Onboard Administrator.

  Redundante OA-Module müssen entsprechend den Anweisungen von HP installiert und konfiguriert sein.
- Stromversorgung.

  Das Gehäuse muss mit ausreichenden Netzteilen gemäß den Empfehlungen in der HP-Dokumentation ausgestattet sein, um einen redundanten Betrieb für die vorgesehene Anzahl von Blades zu ermöglichen.

▸ Vor dem Umkonfigurieren in den ausfallsicheren Modus

Benutzernamen und Kennwörter

Dieser Seite können Sie die Standardbenutzernamen und Kennwörter entnehmen, die von den diversen Komponenten innerhalb Ihres Blade-Servers verwendet werden.

HINWEIS: Falls Sie Kennwörter oder Benutzernamen geändert haben, verwenden Sie diese anstelle der unten angegebenen Standardinformationen.

Komponente	Standardbenutzername	Standardkennwort (bzw. Speicherort des Kennworts)
HP Onboard Administrator	Administrator	Siehe Aufkleber am Gehäuse
HP-Interconnect-Module	admin	admin

Komponente	Standardbenutzername	Standardkennwort (bzw. Speicherort des Kennworts)
HP iLO	(verwaltet über den HP Onboard Administrator)	
Benutzeroberfläche der Email and Web Security-Software	scmadmin	scmchangeme
Konsole der Email and Web Security-Software	support	scmchangeme
Benutzeroberfläche der McAfee Web Gateway-Software	admin	webwasher

▸ Vor dem Umkonfigurieren in den ausfallsicheren Modus

Aktivieren des ausfallsicheren Modus

Nachdem Sie Ihren McAfee® Content Security Blade Server Version 5.6 im Standardmodus (nicht ausfallsicher) installiert und konfiguriert haben, finden Sie in der folgenden Tabelle einen Überblick über die Neukonfiguration des Blade-Servers im ausfallsicheren Modus.

HINWEIS: McAfee empfiehlt, dass Sie den Blade-Server vor der Einrichtung im ausfallsicheren Modus zunächst im Standardmodus (nicht ausfallsicher) betriebsbereit konfigurieren.

Tabelle 7: Übersicht über die Installationsschritte für den ausfallsicheren Modus

Schritt		Beschreibung
1.	Installieren und konfigurieren Sie den Blade-Server im Standardmodus (nicht ausfallsicher), und verifizieren Sie, dass er ordnungsgemäß läuft.	Standardinstallation
2.	Stellen Sie die erforderlichen Informationen über das Netzwerk zusammen.	Vor dem Umkonfigurieren in den ausfallsicheren Modus Hardware-Informationen Benutzernamen und Kennwörter
3.	Sichern Sie die vorhandene Konfiguration.	Sichern der vorhandenen Konfiguration
4.	Erstellen Sie die Basiskonfiguration für die Interconnect-Module.	Konfigurieren der Interconnect-Module
5.	Laden Sie die bearbeiteten Konfigurationsdateien hoch.	Anwenden der Konfiguration für den ausfallsicheren Modus auf alle Interconnect-Module
6.	Laden Sie die generierten Konfigurationsdateien für die Interconnect-Module herunter, und überprüfen Sie sie.	Herunterladen und Überprüfen der generierten Konfiguration
7.	Konfigurieren Sie den Management-Blade-Server für den ausfallsicheren Modus.	Konfigurieren des Management-Blade-Servers für die Verwendung des ausfallsicheren Modus
8.	Nehmen Sie alle erforderlichen Änderungen an der Verkabelung des Blade-Servers vor.	Verbindungen zum externen Netzwerk im ausfallsicheren Modus
9.	Schalten Sie die Blades ein.	Einschalten der Blades

VORSICHT: Wenn Sie den Blade-Server an Ihr Netzwerk anschließen, können der Internetzugang oder andere Netzwerkdienste unterbrochen werden. Planen Sie einen Zeitraum ein, in dem das Netzwerk nicht verfügbar ist, vorzugsweise zu einer Zeit mit geringer Netzwerkauslastung.

Inhalt

- Betrieb im ausfallsicheren Modus
- Sichern der vorhandenen Konfiguration
- Installieren der Interconnect-Module für den ausfallsicheren Modus
- Konfigurieren der Interconnect-Module
- Ändern der Gehäusekonfiguration
- Konfigurieren des Management-Blade-Servers für die Verwendung des ausfallsicheren Modus
- Verbindungen zum externen Netzwerk im ausfallsicheren Modus
- Einschalten der Blades

Sichern der vorhandenen Konfiguration

Gehen Sie wie nachfolgend beschrieben vor, um die vorhandene Konfiguration Ihres McAfee® Content Security Blade Servers zu sichern. Es hat sich bewährt, eine vollständige Sicherung Ihrer Blade-Server-Konfiguration zu erstellen, bevor Sie eine Aktualisierung durchführen, auch dann, wenn Sie vorhaben, eine der Aktualisierungsoptionen zu verwenden, die eine Sicherung und Wiederherstellung Ihrer Konfiguration einschließen.

Vorgehensweise

1. Navigieren Sie in der Benutzeroberfläche zu **System | Cluster-Verwaltung | Konfiguration sichern und wiederherstellen**.
2. Wählen Sie die optionalen Elemente aus, die Sie in die Sicherung aufnehmen möchten (versionsabhängig).
   McAfee empfiehlt, vor der Aktualisierung Ihres Blade-Servers alle Optionen zu sichern.
3. Klicken Sie auf **Konfiguration sichern**.
4. Nach kurzer Zeit wird ein Dialogfeld angezeigt, in dem Sie die gesicherte Konfigurationsdatei auf Ihren lokalen Computer herunterladen können.

- Aktivieren des ausfallsicheren Modus
- Upgrades von früheren Versionen

Installieren der Interconnect-Module für den ausfallsicheren Modus

Bevor Sie Verbindungen aufbauen, müssen Sie die Ethernet-Interconnect-Module installieren und konfigurieren.

Tabelle 8: Legende zu den Abbildungen 9 und 10

#	Beschreibung
1	Anschlüsse für Stromversorgung
2	Interconnect-Module 1 und 2 (verbinden mit LAN 1)
3	Interconnect-Module 3 und 4 (verbinden mit LAN 2)
4	Onboard-Administrator-Anschluss
5	Onboard-Administrator-Modul

#	Beschreibung
6	Out-of-Band-Zugang (Anschluss 20)
7	Out-of-Band (Durchgang) (nur M7)

M3-Gehäuse

Beim M3-Gehäuse werden die Interconnect-Module an der Rückseite des Gehäuses installiert.

Die Interconnect-Module für LAN 1 werden in die Interconnect-Modul-Fächer oben links und oben rechts eingesetzt, die Interconnect-Module für LAN 2 in die Interconnect-Modul-Fächer unten links und unten rechts.

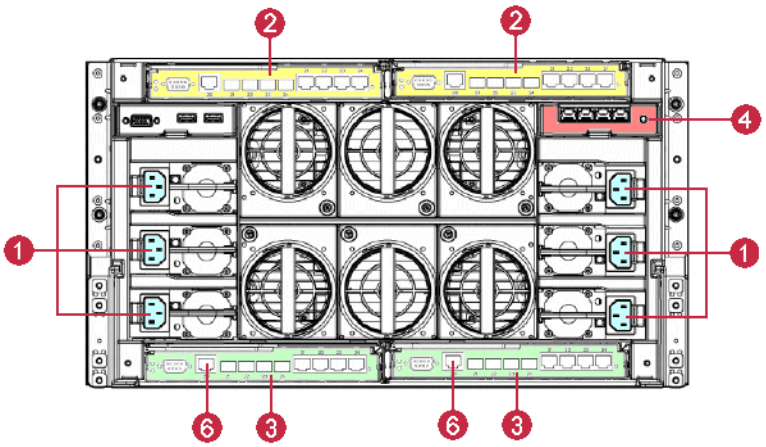


Abbildung 12: M3-Gehäuse – Positionen der Komponenten auf der Rückseite – ausfallsicherer Modus

M7-Gehäuse

Beim M7-Gehäuse werden die Interconnect-Module an der Rückseite des Gehäuses direkt unter der oberen Kühllüfterreihe installiert.

Die Interconnect-Module für LAN 1 werden in die Interconnect-Modul-Fächer oben links und oben rechts eingesetzt, die Interconnect-Module für LAN 2 in die Interconnect-Modul-Fächer direkt darunter.

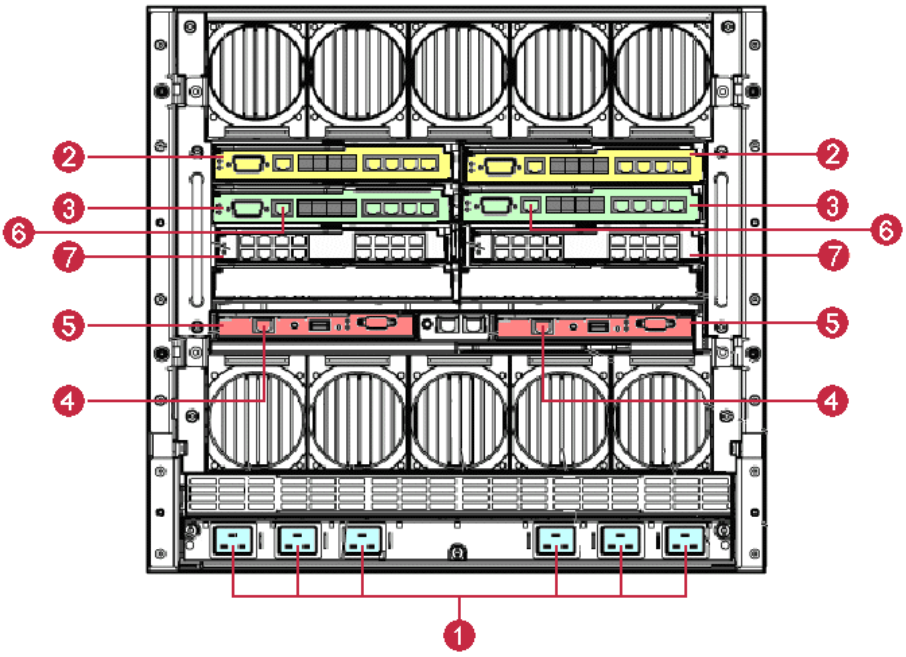


Abbildung 13: M7-Gehäuse – Positionen der Komponenten auf der Rückseite – ausfallsicherer Modus

Führen Sie Folgendes aus:

- Stellen Sie sicher, dass der STP-Status (Spanning Tree Protocol) für die STP-Gruppe 1 "AUS" lautet (standardmäßig sind alle Anschlüsse Mitglieder der STP-Gruppe 1). (Dies gilt, wenn Sie den Blade-Server im Modus "Transparente Bridge" installieren.)
- Konfigurieren Sie die ACLs (Access Control Lists, Zugriffssteuerungslisten) auf den Interconnect-Modulen so, dass die Blade-Server zum Scannen von Inhalten keine externen DHCP-Adressen empfangen können.
- Konfigurieren Sie die ACLs so, dass die Blade-Heartbeat-Pakete im Blade-Server verbleiben.
- Wenn für ein VLAN gekennzeichneter Datenverkehr durch den Blade-Server geleitet werden soll, müssen die Interconnect-Module so konfiguriert werden, dass sie diesen Datenverkehr durchlassen.

Informationen dazu, wie Sie dies tun, finden Sie in der unten aufgeführten Dokumentation:

- HP GbE2c Layer 2/3 Ethernet Blade Switch for c-Class BladeSystem Quick Setup
- HP GbE2c Layer 2/3 Ethernet Blade Switch for c-Class BladeSystem User Guide

In der Tabelle wird dargestellt, welche Interconnect-Module in den einzelnen Gehäusetypen (M3 oder M7) verwendet werden. Standardmäßig können die externen Anschlüsse 21-24 von jedem Interconnect-Modul verwendet werden, um die Netzwerke anzuschließen.

Tabelle 9: Verwendung der Interconnect-Module

	M3-Gehäuse		M7-Gehäuse	
Interconnect-Modul-Fach	**Standardmodus (nicht ausfallsicher)**	**Ausfallsicherer Modus**	**Standardmodus (nicht ausfallsicher)**	**Ausfallsicherer Modus**
1	LAN1	LAN1, SCAN	LAN1	LAN1, SCAN

	M3-Gehäuse		M7-Gehäuse	
Interconnect-Modul-Fach	**Standardmodus (nicht ausfallsicher)**	**Ausfallsicherer Modus**	**Standardmodus (nicht ausfallsicher)**	**Ausfallsicherer Modus**
2	Nicht verwendet	LAN1, SCAN	Nicht verwendet	LAN1, SCAN
3	LAN2	LAN2, OOB	LAN2	LAN2, (OOB)
4	OOB	LAN2, OOB	(OOB)	LAN2, (OOB)
5	----	----	(OOB)	OOB
6	----	----	Nicht verwendet	OOB
7	----	----	Nicht verwendet	Nicht verwendet
8	----	----	Nicht verwendet	Nicht verwendet

Beachten Sie Folgendes:

- Im Standardmodus (nicht ausfallsicher) wird das Scanning-Netzwerk direkt über LAN1 geleitet.
- Im Standardmodus (nicht ausfallsicher) schließen sich die aufgeführten Out-of-Band-Verbindungen (OOB) gegenseitig aus und sind auch nicht ausfallsicher.
- Beim M3-Gehäuse im ausfallsicheren Modus verbindet das Scanning-Netzwerk ungekennzeichnete VLANs über dedizierte Netzwerkkarten innerhalb der Blades.
- Beim M7-Gehäuse im ausfallsicheren Modus nutzt das Scanning-Netzwerk dieselben Netzwerkkarten wie LAN1, der Datenverkehr ist jedoch VLAN-gekennzeichnet, um das Scannen vom LAN1-Datenverkehr zu trennen.
- Im ausfallsicheren Modus ist das Scanning-Netzwerk auf den Scan-Blades ungekennzeichnet, um eine PXE-Installation der Scan-Blades zu ermöglichen.
- Beim M7-Gehäuse werden die Interconnect-Modul-Fächer 5 und 6 von Passthrough-Modulen belegt, die eine direkte Verbindung mit den Management- und Failover-Management-Blade-Servern ermöglichen. Die Scan-Blades verfügen nicht über Out-of-Band-Verbindungen. Dies wird über die Management-Blade-Server und das Scanning-Netzwerk realisiert.
- Standardmäßig ist das Out-of-Band-VLAN als ungekennzeichnet und auf Anschluss 20 aller Interconnect-Module konfiguriert. Sie können Anschluss 20 der Interconnect-Module 1 und 2 verwenden, um mit Ihrem Out-of-Band-Netzwerk die Interconnect-Module des Gehäuses zu verwalten. Anschluss 20 der Interconnect-Module 3 und 4 sind für die Out-of-band-Verwaltung des Email and Web Security-Systems reserviert.

HINWEIS: Bei neuen Installationen und bei Upgrades, bei denen Sie Ihren Blade-Server für den ausfallsicheren Modus konfigurieren, hat sich der LAN2-Anschluss gegenüber früheren Versionen des McAfee Content Security Blade Servers geändert. Bei Standard-Upgrades (nicht ausfallsicher) vorhandener Hardware wird das Interconnect-Modul 2 für den LAN2-Datenverkehr verwendet. Bei neuen Installationen oder bei Upgrades vorhandener Hardware für den ausfallsicheren Modus wird das Interconnect-Modul 3 für den LAN2-Datenverkehr verwendet.

▸ Aktivieren des ausfallsicheren Modus

Konfigurieren der Interconnect-Module

Die Interconnect-Module innerhalb des Blade-Servers müssen konfiguriert werden, damit das Gehäuse im ausfallsicheren Modus betrieben werden kann. Die Email and Web Security-Software übernimmt die Basiskonfigurationen für alle Interconnect-Module und verwendet sie zur

automatischen Generierung der vollständigen Interconnect-Modul-Konfiguration, die für den Betrieb Ihres Blade-Servers im ausfallsicheren Modus benötigt wird.

Die Interconnect-Module innerhalb des Blade-Servers müssen konfiguriert werden, damit das Gehäuse im ausfallsicheren Modus betrieben werden kann. Die Email and Web Security-Software übernimmt die Basiskonfigurationen für die Interconnect-Module und verwendet sie zur automatischen Generierung der vollständigen Interconnect-Modul-Konfiguration, die für den Betrieb Ihres Blade-Servers im ausfallsicheren Modus benötigt wird. Die Methode, mit der die automatisch generierte Konfiguration auf die Interconnect-Module angewendet wird, kann ausgewählt werden:

Tabelle 10: Konfigurationsmethoden

	Verantwortung	Anwendung der Interconnect-Modul-Konfiguration	Bereitgestellte Konfiguration
1.	Benutzer verwaltet Interconnect-Module	Konfigurationsinformationen werden kopiert und in die Interconnect-Modul-CLI eingefügt.	Keine Anmeldeinformationen in der Chassis-Konfiguration. Keine Basiskonfiguration für Interconnect-Module hochgeladen.
2.	Benutzer verwaltet Interconnect-Module	Konfiguration wird benutzergesteuert von der Email and Web Security-Software, einem externen FTP- oder einem TFTP-Server direkt in das Interconnect-Modul heruntergeladen.	Keine Anmeldeinformationen in der Chassis-Konfiguration. Basiskonfigurationsdateien für Interconnect-Module werden in die Email and Web Security-Software hochgeladen.
3.	Benutzer verwaltet Interconnect-Module	Verwenden der Web-Benutzeroberfläche für Interconnect-Module zum Auffinden und Ändern der Konfiguration.	Keine Anmeldeinformationen in der Chassis-Konfiguration. Keine Basiskonfiguration für Interconnect-Module hochgeladen.
4.	Software verwaltet Interconnect-Module	Konfiguration wird bei jeder Änderung von der Email and Web Security-Software direkt in die Interconnect-Module heruntergeladen.	Chassis-Konfiguration enthält Anmeldeinformationen für die Interconnect-Module. Basiskonfigurationsdateien für Interconnect-Module werden in die Email and Web Security-Software hochgeladen.

Unter Beispiel für die Basiskonfiguration eines Interconnect-Moduls und Beispiel einer Chassis-Konfigurationsdatei finden Sie nähere Informationen dazu, welche Informationen in den Basiskonfigurationsdateien für die Interconnect-Modul- und Chassis-Konfigurationsdatei erforderlich sind.

Falls die EWS-Software die Interconnect-Module automatisch konfigurieren soll, gehen Sie wie nachfolgend beschrieben vor, um Basiskonfigurationen für Interconnect-Module zu erstellen.

HINWEIS: Das erforderliche Format für die Interconnect-Modul Basiskonfigurationsdateien ist vom Typ der eingebauten Interconnect-Module abhängig. Für HP GbE2c-Interconnect-Module müssen die Konfigurationsdateien im iscli-Format (wie Cisco IOS) und nicht im HP bladeos-cli-Format generiert werden.

Vorgehensweise

1. Laden Sie die gesamte Konfiguration von jedem Interconnect-Modul mittels FTP oder TFTP auf Ihre Workstation herunter, indem Sie sich bei der Web-Benutzeroberfläche jedes Interconnect-Moduls anmelden oder CLI verwenden.
2. Geben Sie für jedes Interconnect-Modul eindeutige Informationen an. Dazu gehören IP-Adressen, Route-Informationen, Syslog-Server, Zeitserver und Zeitzonen.

3 Entfernen Sie die Konfigurationseinträge für alle Anschlüsse, falls Sie nicht angegeben haben, dass diese Anschlüsse vom Konfigurationsgenerator für Interconnect-Module ignoriert werden sollen.
Dies wird die Basiskonfiguration für jedes Interconnect-Modul.

4 Speichern Sie die Dateien unter /config/resiliency/interconnect.base.*n* (*n* = Interconnect-Modul-Nummer), und fügen Sie sie der gesicherten Konfigurations-ZIP-Datei hinzu.

HINWEIS: Diese gesicherte Konfigurations-ZIP-Datei enthält auch die Datei "chassisconfig.xml", die in Ändern der Gehäusekonfiguration beschrieben wird.

▸ Aktivieren des ausfallsicheren Modus

Ändern der Gehäusekonfiguration

Gehen Sie wie nachfolgend beschrieben vor, um die erforderlichen Änderungen an den Gehäusekonfigurationsdateien vorzunehmen, indem Sie die Datei "chassisconfig.xml" ändern.

Die Datei "chassisconfig.xml" befindet sich innerhalb der Konfigurations-ZIP-Datei, die über **System | Cluster-Verwaltung | Konfiguration sichern und wiederherstellen** gesichert und heruntergeladen werden kann.

Wenn Sie einen Management-Blade-Server das erste Mal installieren, wird eine standardmäßige Version der Datei "chassisconfig.xml" generiert.

Nachdem die Datei "chassisconfig.xml" aktualisiert wurde, wird die Interconnect-Modul-Konfiguration automatisch mit den Anschlusskonfigurationen des Blade-Interconnect-Moduls neu generiert.

Die Elemente innerhalb der Datei "chassisconfig.xml", die höchstwahrscheinlich geändert werden müssen, damit sie Ihren Netzwerkanforderungen entsprechen, sind folgende:

- ScanningVlan (Standard 4094)

  Dies ist die VLAN-ID, die innerhalb des Chassis für das Scanning-Netzwerk verwendet wird.

  Unter normalen Umständen ist dieses VLAN an den externen Anschlüssen des Interconnect-Moduls nicht sichtbar.

  Dieses Netzwerk kann über den symbolischen Namen "scan" an Anschlüsse gebunden werden.

- UntaggedVlan (Standard 4093)

  Dies ist die VLAN-ID, die innerhalb des Chassis für den Transport ungekennzeichneter Rahmen zum externen Netzwerk verwendet wird.

  Dieses Netzwerk kann über den symbolischen Namen "defuntagged" an Anschlüsse gebunden werden.

  Dieses VLAN wird nur innerhalb der Interconnect-Module verwendet. Für den Management-Blade-Server bestimmter Datenverkehr wird mit denselben Tags gekennzeichnet, die auch bei externen Verbindungen vorhanden sind.

- OobVlan (Standard 4092)

  Dies ist die VLAN-ID, die innerhalb des Chassis für die Trennung des OOB-Netzwerks von den anderen Netzwerken innerhalb des Chassis verwendet wird.

  Dieses Netzwerk kann über den symbolischen Namen "oob" an Anschlüsse gebunden werden.

- BridgeVlan (kein Standardwert)

Dies ist eine Liste der VLANs, die im Modus "Transparente Bridge" von LAN1 nach LAN2 überbrückt werden. Es ist nicht erforderlich, VLANs anzugeben, die im EWS-Modus "Transparente Bridge" für das Scannen ausgewählt wurden, da diese automatisch hinzugefügt werden. Die hier angegebenen VLANs werden nicht gescannt, sondern nur von LAN1 nach LAN2 überbrückt.

Dieses Element wird nur dann verwendet, wenn das System im Modus "Transparente Bridge" betrieben wird.

Die Liste der externen VLANs kann über den symbolischen Namen "external" referenziert werden.

- ScanningSTG/ExternalSTG/OobStg

  Dies sind die Konfigurationen für die Spanning-Tree-Gruppen, die für den jeweiligen Spanning Tree des Scanning-Netzwerks, des externen Netzwerks und des OOB-Netzwerks verwendet werden.

  Je nach Topologie des externen Netzwerks und der STG-Konfiguration kann es erforderlich sein, das jeweilige Prioritätsfeld zu ändern.

- Blades

  In diesem Abschnitt sind die Funktionen der einzelnen Blade-Steckplätze aufgeführt. Ein Steckplatz kann als Management-Blade-Server (für den Fall, dass sich die Management-Blade-Server nicht in den Steckplätzen 1 und 2 befinden) oder als zu ignorierender Steckplatz konfiguriert werden. Wenn ein Steckplatz als zu ignorierend konfiguriert wird, wird für die an das Blade angeschlossenen Interconnect-Modul-Anschlüsse keine Konfiguration generiert.

- Interconnect Credentials

  Falls es erforderlich ist, dass die Interconnect-Module ihre Konfiguration automatisch von der EWS-Software erhalten, müssen diese Anmeldeinformationen die richtige IP-Adresse, den richtigen Benutzernamen und das richtige Kennwort enthalten.

  Beachten Sie, dass diese Anmeldeinformationen im Klartext gespeichert werden und daher gelesen werden können, falls das EWS-System kompromittiert werden sollte.

- Interconnect Ports

  Der Betriebsmodus der Interconnect-Modul-Anschlüsse kann hier festgelegt werden. Der wahrscheinlichste Grund zur Änderung der Einstellungen der Interconnect-Modul-Anschlüsse ist es, LACP für die externen Anschlüsse zu aktivieren oder zu deaktivieren oder STP zu aktivieren oder zu deaktivieren. Eine Änderung der Anschlusseinstellungen kann auch erforderlich sein, um externe Anschlüsse für das Scanning-Netzwerk zu reservieren.

  Das VLAN, über das ungekennzeichnete Rahmen die Anschlüsse passieren, wird hier definiert.

  Es kann hilfreich sein, den Anschlüssen aussagekräftige Namen zuzuweisen, wenn die von der Software der Email and Web Security zugewiesenen Namen nicht ausreichend sind.

  Es kann auch angegeben werden, welche Anschlüsse vom Konfigurationsgenerator der Email and Web Security-Software ignoriert werden sollen. Dies verursacht jedoch eine Fehlermeldung, wenn der Konfigurationsgenerator der Email and Web Security-Software eine Konfiguration auf den betreffenden Anschluss einer der Blade-Steckplätze übernehmen muss.

- Interconnect VLANs

  Die Zugehörigkeit der Interconnect-Modul-Anschlüsse zu den VLANs wird hier definiert. VLAN-IDs können numerisch oder – bei den VLANs der Email and Web Security-Software – symbolisch über die oben genannten Namen referenziert werden.

Des Weiteren kann in Erwägung gezogen werden, Folgendes zu konfigurieren:

- das Trunking der externen Interconnect-Modul-Anschlüsse
- die Spanning-Tree-Einstellungen
- der Zugriff auf Ihre Out-of-Band-Management-Netzwerke

In dem Sie die Interconnect-Modul-Anmeldeinformationen und IP-Adressen in die Datei "chassisconfig.xml" aufnehmen, kann die Email and Web Security-Software die Konfigurationen automatisch auf die Interconnect-Module übernehmen.

McAfee empfiehlt jedoch, dies erst zu tun, nachdem Sie verifiziert haben, dass die automatisch generierte Konfiguration ordnungsgemäß funktioniert.

▸ Aktivieren des ausfallsicheren Modus
▸ Anwenden der Konfiguration für den ausfallsicheren Modus auf alle Interconnect-Module
▸ Herunterladen und Überprüfen der generierten Konfiguration

Anwenden der Konfiguration für den ausfallsicheren Modus auf alle Interconnect-Module

Gehen Sie wie nachfolgend beschrieben vor, um die Konfiguration für den ausfallsicheren Modus auf die Interconnect-Module anzuwenden.

Wie in Ändern der Gehäusekonfiguration dargestellt, empfiehlt McAfee, die Interconnect-Modul-IP und die Anmeldeinformationen erst dann in die Konfigurationsdateien einzutragen, wenn Sie die Dateien hochgeladen und geprüft haben, ob die enthaltenen Informationen korrekt sind. Auf diese Weise wird vermieden, dass die Interconnect-Module mit fehlerhaften Informationen konfiguriert werden.

Wenn die Konfigurationsdateien korrekt sind, können Sie die Interconnect-Modul-IP und die Anmeldeinformationen hinzufügen und erneut hochladen. Anschließend werden die Konfigurationsdateien auf die Interconnect-Module angewendet.

Laden Sie die geänderten Konfigurationsdateien auf den Management-Blade-Server, indem Sie eine Konfigurations-ZIP-Datei mit allen geänderten Dateien erstellen und anschließend diese Datei über die Seite **System | Cluster-Verwaltung | Konfiguration sichern und wiederherstellen** wiederherstellen. Dazu gehören:

- Alle Basiskonfigurationsdateien für Interconnect-Module.
- Die Datei "chassisconfig.xml".

Sie müssen die Änderungen übernehmen, damit der Blade-Server die hochgeladene Konfiguration verwenden kann.

HINWEIS: Falls Sie die Anmeldeinformationen und IP-Adressen für Interconnect-Module in die Gehäusekonfigurationsdatei (chassisconfig.xml) aufgenommen haben, wird die Konfiguration für den ausfallsicheren Modus automatisch auf jedes Interconnect-Modul angewendet.

▸ Ändern der Gehäusekonfiguration

Herunterladen und Überprüfen der generierten Konfiguration

Laden Sie die generierten Konfigurationsdateien "interconnect_config.X.n" herunter und prüfen Sie sie, um sicherzustellen, dass die generierte Konfiguration Ihren Vorstellungen entspricht.

Diese werden unter **System | Cluster-Verwaltung | Ausfallsicherer Modus** angezeigt.

Sollten diese Dateien fehlerhaft sein, wiederholen Sie die Schritte zum Definieren und Generieren der Konfiguration, um diese Probleme zu beheben.

▸ Ändern der Gehäusekonfiguration

Konfigurieren des Management-Blade-Servers für die Verwendung des ausfallsicheren Modus

Gehen Sie wie nachfolgend beschrieben vor, um den Management-Blade-Server für die Verwendung des ausfallsicheren Modus zu konfigurieren.

Vorgehensweise

1. Navigieren Sie in der Benutzeroberfläche zu **System | Cluster-Verwaltung | Ausfallsicherer Modus**.
2. Klicken Sie auf **Ausfallsicheren Modus aktivieren**.
3. Klicken Sie zur Bestätigung, dass Sie die **Warnung beim Aktivieren des ausfallsicheren Modus** verstanden haben, auf **OK**.
4. Warten Sie darauf, dass der Management-Blade-Server, der Failover-Management-Blade-Server und alle Scan-Blades automatisch herunterfahren.
5. Nehmen Sie alle erforderlichen Änderungen an den Interconnect-Modulen für die Verbindung eines externen Netzwerkes mit den Blade-Servern vor.
6. Schließen Sie den Management-Blade-Server und den Failover-Management-Blade-Server an die Stromversorgung an.
   Überprüfen Sie im Dashboard, ob der Management- und der Failover-Management-Blade-Server ordnungsgemäß funktionieren und ob die Synchronisierung stattgefunden hat.
7. Schalten Sie der Reihe nach alle Blade-Server zum Scannen von Inhalten ein.

▸ Aktivieren des ausfallsicheren Modus

Verbindungen zum externen Netzwerk im ausfallsicheren Modus

Die Verbindungen, die Sie zwischen Ihrem externen Netzwerk und Ihrem McAfee® Content Security Blade Server benötigen, hängen vom Betriebsmodus ab, den Sie für den Blade-Server ausgewählt haben, sowie von der Konfiguration des externen Netzwerks.

Wenn Sie den Onboard Administrator (OA) verwenden, stellen Sie sicher, dass Sie Verbindungen zum OA sowie zu den Interconnect-Modulen haben.

Stellen Sie sicher, dass alle Verbindungen zwischen dem Netzwerk und den Interconnect-Modulen des Blade-Servers aus gebündelten Verbindungen bestehen, um Ausfallsicherheit für den Fall zu bieten, dass ein Switch, ein Interconnect-Modul oder ein Kabel ausfällt.

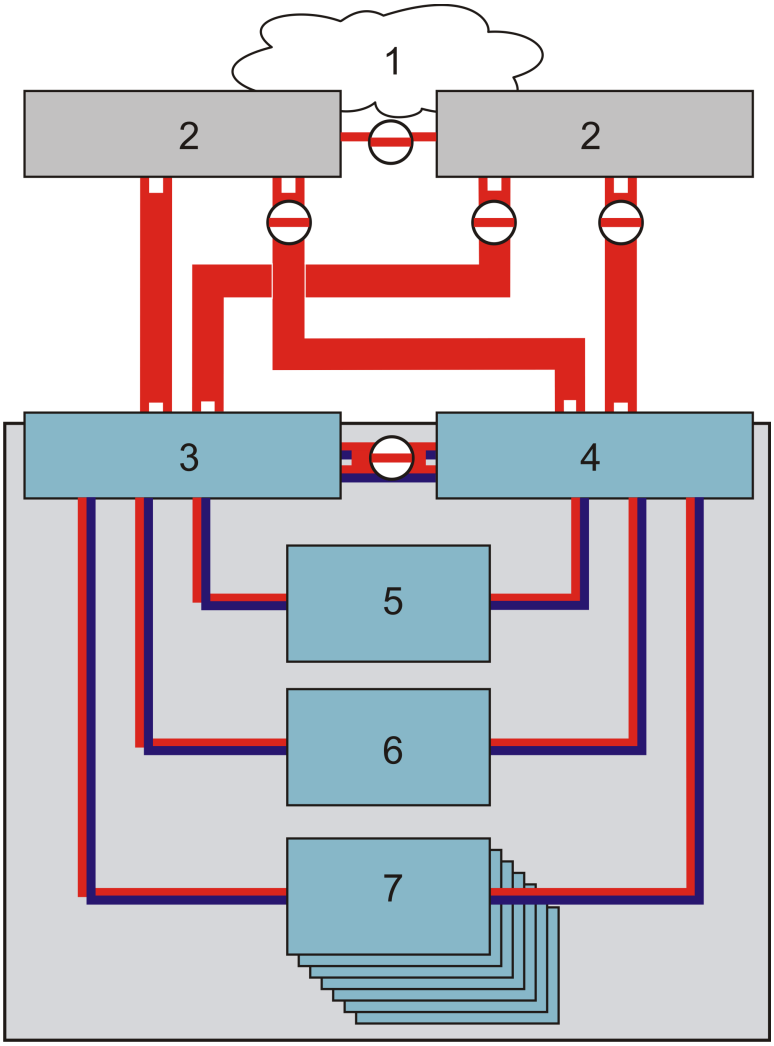


Abbildung 14: Typische Netzwerkverbindungen - ausfallsicherer Modus

Tabelle 11: Schlüssel

	LAN-Verbindungen (LAN1, LAN2 oder OOB)
	Internes Scanning-Netzwerk
	Gebündelte Verbindungen
	Von STP normalerweise blockierte Verbindungen
1	Externes Netzwerk
2	Netzwerkinfrastruktur
3	(für LAN1) Interconnect-Modul 1, (für LAN2 oder OOB) Interconnect-Modul 3
4	(für LAN1) Interconnect-Modul 2, (für LAN2 oder OOB) Interconnect-Modul 4
5	Management-Blade-Server

6	Failover-Management-Blade-Server
7	Scan-Blades

HINWEIS: Zwecks einfacherer Darstellungen wird im Diagramm nur ein Satz von LAN/OOB-Pfaden gezeigt. Die Pfade für LAN1, LAN2 und OOB sind ähnlich.

▸ Aktivieren des ausfallsicheren Modus

Einschalten der Blades

Gehen Sie wie nachfolgend beschrieben vor, um alle Blades in Ihrem McAfee® Content Security Blade Server einzuschalten.

Vorbereitung

Stellen Sie sicher, dass Sie alle Aufgaben aus dem Abschnitt Aktivieren des ausfallsicheren Modus dieses Handbuchs durchgeführt haben.

Vorgehensweise

1. Drücken Sie die Netzschalter am Management-Blade-Server.
2. Wenn der Management-Blade-Server die Startsequenz abgeschlossen hat, drücken Sie den Netzschalter des Failover-Management-Blade-Servers.
3. Nachdem der Management-Blade-Server und Failover-Management-Blade-Server ihre Startsequenzen abgeschlossen haben, können Sie die Blade-Server zum Scannen von Inhalten einschalten.

   HINWEIS: Zur Vermeidung von Spannungsspitzen empfiehlt McAfee, dass Sie warten, bis jedes Scan-Blade die Startsequenz abgeschlossen hat, bevor Sie den nächsten Blade-Server zum Scannen von Inhalten einschalten.

▸ Aktivieren des ausfallsicheren Modus

Fehlerbehebung

In diesem Abschnitt werden einige der Probleme erläutert, die beim Integrieren Ihres Geräts in das bereits vorhandene Netzwerk auftreten können.

Wählen Sie in der Navigationsleiste **Fehlerbehebung** aus, um das Fehlerbehebungstool zu verwenden.

Häufig gestellte Fragen (FAQs)

- Blade-spezifische Fehlerbehebung
- Systemkonfiguration
- Anti-Spam
- Automatische Aktualisierung der Antiviren-Software
- Zustellung
- Die Directory Harvest-Prävention funktioniert nicht
- E-Mail-Anhänge
- ICAP
- E-Mail-Probleme
- POP3
- Allgemeine Probleme
- Systemverwaltung
- Weitere Hilfe – Die Link-Leiste

Blade-spezifische Fehlerbehebung

Die folgenden Themen enthalten spezielle Informationen für die Fehlerbehebung bei Ihrem McAfee® Content Security Blade Server.

- Externe Überwachungssysteme
- Status der Netzwerkkarte
- Systemereignisse

Externe Überwachungssysteme

McAfee empfiehlt, ein dediziertes Überwachungssystem zu konfigurieren, das zusätzliche Warnungsmeldungen zu Problemen oder Fehlern innerhalb der Content Security Blade Server-Gehäuse liefert.

Der Zustand des Gehäuses und der Interconnect-Module kann mithilfe des SNMP-Protokolls direkt überwacht werden. Außerdem können die integrierten Lights-Out-Module so konfiguriert

werden, dass sie SNMP-Traps senden, falls Fehlerzustände festgestellt werden. Die Email and Web Security-Software kann ebenfalls mittels SNMP überwacht werden.

Status der Netzwerkkarte

Der Status der Verbindungen zu allen Netzwerkkarten auf jedem Blade ist über die Benutzeroberfläche der Email and Web Security Appliance-Software verfügbar und wird auf der Seite **System | Cluster-Verwaltung | Lastenausgleich** angezeigt.

Systemereignisse

Verwenden Sie innerhalb der Benutzeroberfläche der Email and Web Security Appliance-Software **Berichte | Systemberichte**, um Informationen des Blade-Überwachungssystems und des Konfigurationssystems für die Interconnect-Module abzurufen.

Systemkonfiguration

Ich habe das FTP-Protokoll deaktiviert, aber meine Benutzer können FTP weiterhin mit ihren Browsern verwenden

Überprüfen Sie die FTP-Proxy-Einstellungen des Browsers. Wählen Sie in Internet Explorer **Extras | Internetoptionen | Verbindungen | LAN-Einstellungen | Proxyserver | Erweitert**.

Die Appliance kann FTP über ihren HTTP-Protokoll-Handler unterstützen. Wenn also der FTP-Proxy für Port 80 eingerichtet ist, können Ihre Benutzer noch immer FTP verwenden.

HINWEIS: Dies gilt nur für FTP-Downloads. Die Appliance unterstützt keine FTP-Uploads über HTTP.

Transparente Web-Authentifizierung

Wie konfiguriere ich die transparente Web-Authentifizierung mit Kerberos?

Wenn Sie auf einem Blade-Server die transparente Web-Authentifizierung mit Kerberos konfigurieren, müssen Sie sich jeweils beim Management-Blade-Server und beim Failover-Management-Blade-Server anmelden und auf beiden Kerberos konfigurieren. Dies ist notwendig, da die Authentifizierungsdaten aus folgenden Gründen nicht automatisch zwischen dem Management-Blade-Server und dem Failover-Management-Blade-Server synchronisiert werden können:

Bei der Verwendung des Modus "Transparente Bridge" kann kein Keytab erstellt werden, das sowohl auf dem Management-Blade-Server als auch auf dem Failover-Management-Blade-Server funktioniert.

Dies liegt daran, dass das Keytab den Host-Namen des Blade-Servers enthält, der entweder in die IP-Adresse für den Management-Blade-Server oder in die IP-Adresse des Failover-Management-Blade-Servers aufgelöst wird.

Um Kerberos für den Betrieb im Modus "Transparente Bridge" zu konfigurieren, müssen Sie zwei Keytabs erstellen, eines, das die IP-Adresse und den Host-Namen des Management-Blade-Servers enthält, und eines, das die IP-Adresse und den Host-Namen des

Failover-Management-Blade-Servers enthält. Importieren Sie die beiden Keytabs in den entsprechenden Management-Blade-Server.

HINWEIS: Dieses Problem besteht in den Modi "Expliziter Proxy" und "Transparenter Router" nicht, da der Blade-Server für den gerade aktiven Management-Blade-Server eine virtuelle IP-Adresse verwendet.

Wie konfiguriere ich die transparente Web-Authentifizierung mit NTLM?

Wenn Sie die transparente Web-Authentifizierung mit NTLM auf einem Blade-Server konfigurieren, müssen Sie sich jeweils beim Management-Blade-Server und beim Failover-Management-Blade-Server anmelden und auf beiden NTLM konfigurieren. Dies ist notwendig, da die Authentifizierungsdaten aus folgenden Gründen nicht automatisch zwischen dem Management-Blade-Server und dem Failover-Management-Blade-Server synchronisiert werden können:

Für die Authentifizierung mit NTLM müssen der Benutzername und das Kennwort eingegeben werden, damit der Blade-Server eine Verbindung zum NTLM-Domänencontroller herstellen kann. Aus Sicherheitsgründen werden der Benutzername und das Kennwort nicht auf dem Blade-Server gespeichert.

Sie müssen sich einzeln beim Management-Blade-Server und beim Failover-Management-Blade-Server anmelden und eine Verbindung zum Domänencontroller herstellen. In beiden Fällen müssen Sie den Benutzernamen und das Kennwort nur bei der anfänglichen Konfiguration eingeben.

HINWEIS: McAfee empfiehlt, dass Sie sich nach dem Konfigurieren des Management-Blade-Servers beim Failover-Management-Blade-Server anmelden. Auf der Oberfläche wird eine Warnmeldung angezeigt, die Sie daran erinnert, das Keytab zu importieren oder dem NTLM-Domänencontroller beizutreten.

Anti-Spam

Ich habe die Appliance so konfiguriert, dass Spam-Mail durch eine RBL-Server-Überprüfung abgelehnt wird, aber einige Spam-Mails kommen dennoch an.

Es gibt keine Anti-Spam-Software, die sämtliche Spam-E-Mails erkennen und blockieren kann. Die Appliance verwendet eine Liste der Namen von bekannten Personen, die E-Mail-Missbrauch betreiben, sowie der von ihnen benutzten Netzwerke. Diese Listen verringern die Anzahl unerwünschter E-Mails zwar wirksam, sind aber nicht vollständig.

Um einen bestimmten Spam-Absender zu blockieren, fügen Sie die E-Mail-Adresse des Absenders zur Liste **Verweigerte Absender** hinzu.

E-Mail | E-Mail-Konfiguration | Empfangen von E-Mails | Listen für Zulassen und Verweigern | Zugelassene und blockierte Absender

Benutzer erhalten keine normalen E-Mail-Nachrichten

Benutzer empfangen möglicherweise aus folgenden Gründen keine regulären E-Mail-Nachrichten:

- Die E-Mail-Nachrichten könnten von einem Absender stammen, der in der Liste **Blockierte Absender** aufgeführt ist. Sie müssen möglicherweise Folgendes durchführen:

  - Die Liste **Blockierte Absender** genauer definieren, um zu gewährleisten, dass erwünschte E-Mail-Nachrichten nicht blockiert werden. Es ist beispielsweise sinnvoller, eine bestimmte E-Mail-Adresse einzugeben, als eine gesamte Domäne oder ein gesamtes Netzwerk zu sperren.
  - Fügen Sie der Liste **Zugelassene Absender** den Absender, die Domäne oder das Netzwerk hinzu. Die Appliance scannt keine E-Mails von Absendern, Domänen und Netzwerken, die sich in dieser Liste befinden, auf Spam. Die Liste **Zugelassene Absender** hat Vorrang vor Einträgen in der Liste **Blockierte Absender**.
- Die E-Mail-Nachricht wurde vielleicht blockiert, weil sie von einem Absender oder einem Unternehmen stammt, der bzw. das von einer Echtzeit-Anti-Spam-Liste als potenzielle Spam-Quelle erkannt wurde.
- Das Verhältnis zwischen blockierten Spam- und regulären E-Mail-Nachrichten muss möglicherweise korrigiert werden. Wenn die Appliance beispielsweise selbst E-Mail-Nachrichten mit einem nur geringen Spam-Risiko blockiert, laufen Sie Gefahr, versehentlich auch normale E-Mail-Nachrichten zu blockieren. Es ist sinnvoller, eine gewisse Anzahl von Spam-Mails zuzulassen.
- Die E-Mail-Nachricht könnte einen Virus oder ein potenziell unerwünschtes Programm enthalten und wurde durch einen Virenscanner blockiert.

E-Mail | E-Mail-Konfiguration | Empfangen von E-Mails | Listen für Zulassen und Verweigern

Benutzer erhalten weiterhin Spam

Benutzer empfangen möglicherweise aus folgenden Gründen weiterhin Spam:

- Keine Anti-Spam-Software kann alle E-Mail-Nachrichten blockieren, die Spam enthalten könnten. Um Spam optimal erkennen und diesbezüglich Gegenmaßnahmen ergreifen zu können, stellen Sie sicher, dass die Appliance stets mit den aktuellsten Versionen des Anti-Spam-Moduls, der Anti-Spam-Regeln und zusätzlichen Regeldateien arbeitet. Lesen Sie auch *Absenderauthentifizierung und Reputation*, um sicherzustellen, dass Sie alle Funktionen nutzen, die unerwünschte E-Mail blockieren können.
- Die Appliance lässt das Passieren von Stream-Medien zu.

  Das Passieren von Stream-Medien stellt ein Sicherheitsrisiko dar, da Stream-Medien nicht von der Appliance gescannt werden. Es wird davon abgeraten, dass Stream-Medien des Typs *application/octet-stream* oder *application/** die Appliance passieren können, da diese MIME-Typen ausführbar sind und ein hohes Sicherheitsrisiko darstellen.
- Sie müssen möglicherweise eine strengere Anti-Spam-Richtlinie einrichten. Möglicherweise möchten Sie z. B. mehr E-Mail-Nachrichten als Spam markieren, bevor diese von den Benutzern empfangen werden, oder einfach Spam auf der Appliance-Ebene blockieren.
- Die E-Mail-Nachrichten könnten von Absendern, Domänen oder Netzwerken stammen, die in der Liste **Zugelassene Absender** aufgeführt sind. Überprüfen Sie die Liste, um sicherzugehen, dass E-Mail-Nachrichten von diesen Absendern wirklich vom Anti-Spam-Scan ausgenommen werden sollen. Möglicherweise sollten Sie die Einträge der Liste genauer definieren. Geben Sie beispielsweise einzelne E-Mail-Adressen an, statt ganze Domänen oder Netzwerke zuzulassen. Siehe die Liste **Zugelassene Absender**.
- Die E-Mail-Client-Software verschiebt unerwünschte Nachrichten nicht automatisch in einen Spam-Ordner. Benutzer sehen also weiterhin Spam-Nachrichten in ihrem Posteingang.

Weitere Informationen zum Einrichten von Mail-Clients finden Sie unter *Konfigurieren von Mail-Clients*.

- Die E-Mail-Nachricht könnte größer sein als zulässig, weshalb sie nicht auf Spam gescannt wird. Siehe zur Größenänderung die erweiterten Optionen in den Anti-Spam-Einstellungen.
- Die E-Mail-Nachrichten werden nicht über eine Appliance geroutet, auf der die Anti-Spam-Software aktiviert ist.

E-Mail | E-Mail-Konfiguration | Empfangen von E-Mails

Wie kann ein bestimmter Typ von Spam gestoppt werden?

Ihr Blade-Server aktualisiert sein Anti-Spam-Modul und seine Spam-Erkennungsregeln regelmäßig.

Überprüfen Sie Folgendes, um die optimale Erkennung und Vermeidung von Spam sicherzustellen:

- Die Appliance nutzt die neuesten Versionen des Anti-Spam-Moduls und der Anti-Spam-Regeln.
- Die Appliance wurde so konfiguriert, dass Stream-Medien die Appliance nicht passieren können.

System | Komponentenverwaltung | Aktualisierungsstatus

Benutzer klagen über volle Posteingänge

Wenn Benutzer Spam automatisch in einen Spam-Ordner im Posteingang umleiten, kann ihr Posteingang rasch sein Größenlimit überschreiten. Erinnern Sie die Benutzer daran, regelmäßig ihre Spam-Ordner zu überprüfen und Spam zu löschen.

Automatische Aktualisierung der Antiviren-Software

Wenn ich eine sofortige Aktualisierung anfordere, geschieht nichts. Wie kann ich erkennen, ob die DAT-Datei aktualisiert wurde?

Die DAT-Dateien werden heruntergeladen, überprüft und angewendet – nicht einfach nur hinzugefügt. Die Appliance wartet nicht, bis die Aktualisierung abgeschlossen ist, sondern startet im Hintergrund. Die Aktualisierung kann einige Minuten in Anspruch nehmen, sogar mit einer schnellen Internetverbindung.

Sie sehen die Versionsnummer der installierten DAT-Dateien, kurz nachdem die Appliance die neuen DAT-Dateien erfolgreich installiert hat.

System | Komponentenverwaltung | Aktualisierungsstatus

Dashboard | Systemstatus – Updates

Zustellung

Welche Einstellungen kann ich überprüfen, wenn Probleme bei der E-Mail-Zustellung auftreten?

Falls Ihr interner Mail-Server keine eingehenden E-Mails empfängt, überprüfen Sie, ob dieser Mail-Server so konfiguriert ist, dass er E-Mails von der Appliance akzeptiert.

Geben Sie in der Liste der lokalen Domänen für die E-Mail-Zustellung keine allgemeine Regel mit Platzhaltern an. Aktivieren Sie stattdessen das Fallback-Relay, und legen Sie sie dort fest.

E-Mail | E-Mail-Konfiguration | Empfangen von E-Mails | Anti-Relay-Einstellungen

Die Directory Harvest-Prävention funktioniert nicht

Damit die Directory Harvest-Prävention ordnungsgemäß funktioniert, muss der E-Mail-Server während der SMTP-Kommunikation eine Überprüfung auf gültige Empfänger durchführen und anschließend einen Non-Delivery-Report senden.

Einige E-Mail-Server senden keine Fehler vom Typ "Unbekannter Benutzer" als Teil der SMTP-Konfiguration. Dazu gehören u. a. die folgenden Server:

- Microsoft Exchange 2000 und 2003 (wenn die Standardkonfiguration verwendet wird)
- qmail
- Lotus Domino

Schlagen Sie in der Benutzerdokumentation des E-Mail-Servers nach, ob der E-Mail-Server so konfiguriert werden kann, dass er den Bericht "550 Recipient address rejected: User unknown" (Empfängeradresse nicht akzeptiert: Unbekannter Benutzer) als Teil der SMTP-Kommunikation sendet, wenn eine Nachricht an einen unbekannten Benutzer gefunden wird.

Mit der LDAP-Integration kann dieses Problem umgangen werden.

E-Mail-Anhänge

Die Appliance blockiert alle E-Mails, wenn ich die Anzahl der Anhänge verringere, ab der blockiert werden soll.

Diese Einstellung soll E-Mail-Nachrichten mit einer großen Zahl von Anhängen blockieren, die zu viel Bandbreite belegen.

Einige E-Mail-Clients (z. B. Outlook Express) speichern zusätzliche Informationen in zusätzlichen Anhängen und betten sogar den Hauptnachrichtentext in einen Anhang ein.

Wenn diese Zahl zu niedrig gewählt ist, werden u. U. sogar reguläre E-Mail-Nachrichten abgelehnt.

E-Mail | E-Mail-Richtlinien | Scan-Richtlinien | Filterung nach Mailgröße | Anhangszähler

EICAR (der Testvirus) oder Inhalt, der blockiert werden muss, gelangt immer noch durch.

Stellen Sie sicher, dass sich die Appliance wirklich im Mail-Pfad befindet. Untersuchen Sie die Header einer E-Mail-Nachricht (wählen Sie in Outlook **Ansicht | Optionen | Internetkopfzeilen**).

Wenn sich die Appliance im Mail-Pfad befindet, wird ein Header der Form **Received: from Absender by Appliancename via ws_smtp** angezeigt, wobei **Absender** und **Appliancename** durch den Namen des tatsächlichen Absenders und den Namen der Appliance ersetzt werden.

Wenn die Appliance einen Virus erkennt, erhalte ich eine Benachrichtigung über eine Inhaltsverletzung

Dieses Problem kann durch einen Konflikt zwischen der Warnhinweisseite der HTML-Vorlage und einer Inhalts-Scan-Regel verursacht werden.

Es kann dann auftreten, wenn Sie beispielsweise den Inhalt nach dem Wort **Virus** filtern, gleichzeitig aber die HTML-Vorlage für die Virenerkennung so eingerichtet haben, dass sie die Warnung **Ein Virus wurde erkannt** ausgibt. Eine eingehende Nachricht mit einem Virus bewirkt, dass die Nachricht durch die Meldung **Ein Virus wurde erkannt** ersetzt wird. Die Ersatzmeldung läuft daraufhin durch den Inhaltsfilter, der durch das Wort **Virus** ausgelöst wird, und die Meldung wird dann durch eine Inhaltsverletzung anstelle einer Virenbenachrichtigung ersetzt.

E-Mail | E-Mail-Richtlinien | Scan-Richtlinien

Die Appliance reagiert langsam, wenn ich mich an der Benutzeroberfläche anmelde

Stellen Sie sicher, dass der Browser, mit dem Sie die Verbindung herstellen, nicht die Appliance selbst als Proxy verwendet. Gehen Sie im Internet Explorer zu **Extras | Internetoptionen | Verbindungen | LAN-Einstellungen**, und deaktivieren Sie **Proxyserver verwenden**.

Überprüfen Sie das DNS-Setup auf der Appliance. Das Feld "DNS-Server" muss die IP-Adresse eines gültigen DNS-Servers enthalten, auf den die Appliance zugreifen können muss.

Wenn die Appliance stark belastet ist, verlangsamt sich die Reaktionszeit der Benutzeroberfläche. Erwägen Sie die Verwendung der Out-of-Band-Verwaltung.

System | Appliance-Verwaltung | DNS und Routing

System | Appliance-Verwaltung | Remote-Zugriff | Out-of-Band-Verwaltung

ICAP

ICAP-Dienst nicht gefunden

In diesem Abschnitt wird ein verbreitetes Konfigurationsproblem beschrieben, das auftritt, wenn ICAP-Dienste eingerichtet oder umkonfiguriert werden.

Wenn der ICAP-Client den angeforderten Dienst nicht findet:

- Prüfen Sie, ob der ICAP-Client einen gültigen Dienst anfordert. Beim Konfigurieren des ICAP-Clients passiert es schnell, dass der Pfad des Dienstes fehlerhaft eingegeben wird. Dienstpfade beginnen mit einem Schrägstrich (/) und unterscheiden zwischen Groß- und Kleinschreibung. Stellen Sie sicher, dass Sie den exakten Pfadnamen angegeben haben. Beispiel: Der Pfad /REQMOD unterscheidet sich vom Pfad /REQMOD/.
- Prüfen Sie, ob die Appliance den gewünschten ICAP-Dienst unterstützt und ob der angeforderte Dienst auf der Appliance nicht deaktiviert wurde.

  HINWEIS: Einige ICAP-Server unterstützen nicht alle ICAP-Verben. Beispiel: Einige ICAP-Clients unterstützen nur das Verb REQMOD. Die Appliance unterstützt standardmäßig die Verben REQMOD, RESPMOD und OPTIONS. Die Dienste REQMOD und RESPMOD können jedoch in der Appliance deaktiviert sein.

- Prüfen Sie, ob die Netzwerkverbindung zwischen dem ICAP-Client und dem ICAP-Server funktioniert. Verwenden Sie einen Ping-Test.

Fehlerbehebung | Tools | Ping- und Traceroute

Appliance-Verbindungen nicht verfügbar

Wenn die Appliance keine verfügbaren Verbindungen mehr hat, kann es erforderlich sein, das ICAP-Protokoll neu zu starten.

Erläuterung der ICAP-Statuscodes

Diese Liste der ICAP-Statuscodes entspricht dem Stand zum Zeitpunkt der Veröffentlichung. Wenn ein Statuscode nicht in der Tabelle enthalten ist, finden Sie die aktuellsten Informationen im ICAP-RFC-Standard.

Tabelle 12: ICAP-Statuscodes

Code	Beschreibung
100	Continue after ICAP preview (Nach ICAP-Vorschau fortsetzen).
200	OK. Die Appliance versteht die Anfrage und antwortet.
204	No modifications needed (Keine Änderungen erforderlich) (teilweise auch als 204 No Content [204 "Kein Inhalt"] bekannt).
400	Bad request (Falsche Anfrage).
404	ICAP service was not found (ICAP-Dienst nicht gefunden).
405	The method not allowed for this service (Methode für Dienst nicht zulässig). Beispiel: Eine RESPMOD-Anfrage für einen Dienst, der nur REQMOD unterstützt.
408	Request has timed-out (Zeitlimit für die Anfrage überschritten). ICAP-Server wartet nicht länger auf eine Anfrage eines ICAP-Clients.
500	ICAP server error (ICAP-Server-Fehler). Beispiel: Der ICAP-Server verfügt nicht mehr genügend freien Speicher.
501	Method (verb) not implemented (Methode [Verb] nicht implementiert).
502	Bad Gateway (Falsches Gateway).
503	Service overloaded (Dienst überlastet). Der ICAP-Server hat die dem Dienst zugewiesene maximale Anzahl an Verbindungen überschritten. Der ICAP-Client darf diese Grenze nicht überschreiten.

Code	Beschreibung
505	ICAP version not supported by the ICAP server (ICAP-Version wird vom ICAP-Server nicht unterstützt).

E-Mail-Probleme

Warum kann ich nicht nur den Namen des Absenders angeben, für den ich das Relay blockieren möchte?

Sie müssen sich das Anti-Relay als eine Blockierung zwischen zwei Systemen vorstellen, Anti-Spam hingegen als eine absenderbasierte Blockierung.

Das Anti-Relay wird mithilfe der Domänen und Netzwerke konfiguriert, für die die Appliance E-Mails überträgt. Die Anti-Spam-Konfiguration blockiert eine Nachricht jedoch basierend auf deren Absender.

E-Mail | E-Mail-Konfiguration | Empfangen von E-Mails | Anti-Relay-Einstellungen | Weiterleiten der E-Mail

E-Mail | E-Mail-Richtlinien | Scan-Richtlinien | Spam

Die Directory Harvest-Prävention funktioniert nicht

Damit die Directory Harvest-Prävention ordnungsgemäß funktioniert, muss der E-Mail-Server während der SMTP-Kommunikation eine Überprüfung auf gültige Empfänger durchführen und anschließend einen Non-Delivery-Report senden.

Einige E-Mail-Server senden keine Fehler vom Typ **Unbekannter Benutzer** als Teil der SMTP-Konfiguration. Dazu gehören u. a. die folgenden Server:

- Microsoft Exchange 2000 und 2003, wenn die Standardkonfiguration verwendet wird.
- qmail
- Lotus Domino

Schlagen Sie in der Benutzerdokumentation des E-Mail-Servers nach, ob der E-Mail-Server so konfiguriert werden kann, dass er den Bericht **550 Recipient address rejected: User unknown** (Empfängeradresse nicht akzeptiert: Unbekannter Benutzer) als Teil der SMTP-Konversation sendet, wenn eine Nachricht an einen unbekannten Benutzer gefunden wird.

Mit der LDAP-Integration kann dieses Problem umgangen werden.

E-Mail | E-Mail-Konfiguration | Empfangen von E-Mails | Empfängerauthentifizierung | Directory Harvest-Prävention

Replikation zwischen Mail-Servern funktioniert nicht

Wenn sich die Appliance zwischen zwei Microsoft Exchange-Servern befindet, müssen Sie sicherstellen, dass die Appliance die ESMTP-E-Mail-Header (Extended SMTP) nicht blockiert.

Lassen Sie die Verwendung aller ESMTP-Erweiterungen zu: X-EXPS, X-LINK2STATE, XEXCH50 und CHUNKING.

E-Mail | E-Mail-Konfiguration | Protokollkonfiguration | Protokolleinstellungen | Transparenzoptionen | Erweiterte Optionen

POP3

Ich habe eine dedizierte POP3-Verbindung eingerichtet, und POP3 funktioniert nicht mehr

Der allgemeine und der dedizierte Server dürfen nicht denselben Port verwenden. Die Standard-Port-Nummer für POP3 lautet 110. Der dedizierte Server setzt den allgemeinen Server außer Kraft.

E-Mail | E-Mail-Konfiguration | Protokollkonfiguration | Protokolleinstellungen | POP3-Protokolleinstellungen

Wenn ich E-Mails mit Outlook Express über POP3 abrufe, erhalte ich manchmal eine Zeitüberschreitungsmeldung mit der Option "Abbrechen" oder "Warten"

Die Appliance muss die gesamte E-Mail-Nachricht herunterladen und scannen, bevor sie sie an Outlook Express weiterleiten kann. Bei einer großen Nachricht oder einem langsamen E-Mail-Server kann dies einige Zeit in Anspruch nehmen. Klicken Sie auf **Warten**, um Outlook Express zum Warten zu zwingen, bis die Appliance die Nachricht verarbeitet hat.

Ich erhalte gelegentlich POP3-Mail-Nachrichten doppelt

Einige E-Mail-Clients gehen nicht korrekt mit Zeitüberschreitungen um. Wenn die Appliance eine sehr große Nachricht herunterlädt und scannt, kann beim Client während des Wartens auf eine Antwort eine Zeitüberschreitung eintreten.

In einem Popup-Fenster werden Sie aufgefordert, zu warten oder das Herunterladen abzubrechen. Wenn Sie **Abbrechen** wählen und einen zweiten Download starten, kann sich die Nachricht zwei Mal in Ihrem Posteingang befinden.

Allgemeine Probleme

Die Browser-Schaltfläche "Zurück" bringt mich nicht zur vorherigen Seite zurück.

Dies ist ein bekanntes Problem bei Webbrowsern. McAfee empfiehlt, in der oberen rechten Ecke der Appliance-Oberfläche auf den Rückwärtspfeil zu klicken.

Systemverwaltung

Die Appliance nimmt die HotFix-Datei nicht an

Dekomprimieren Sie die HotFix-Datei nicht, bevor Sie sie auf die Appliance hochladen. Die Appliance akzeptiert die Originaldatei so, wie Sie sie empfangen haben – nämlich mit der Erweiterung ZIP.

System | Komponentenverwaltung | Paketinstallationsprogramm

Wie kann ich die Größe der Protokolldateien der Appliance steuern?

Die Appliance speichert ihre Protokolldateien in einem textähnlichen Format (XML) auf einer Partition (/log) ihrer internen Festplatte. Standardmäßig werden die Protokolle nach einigen Tagen geleert. Die Appliance gibt eine Warnung aus, wenn ihre Bereiche beinahe gefüllt sind, in der Regel bei 75 % und bei 90 %.

McAfee empfiehlt Folgendes:

- Ermitteln Sie die prozentuale Belegung der Protokollpartition.
- Beschränken Sie die Größe der Protokolldatei, und erstellen Sie regelmäßig Sicherungskopien der Protokolldatei.
- Passen Sie die Warnstufen an.

Fehlerbehebung | Tools | Speicherplatz

System | Cluster-Verwaltung | Konfiguration sichern und wiederherstellen

Dashboard | Systemstatus | Bearbeiten

Weitere Hilfe – Die Link-Leiste

Die Link-Leiste im Benutzeroberflächen-Fenster der Appliance bietet Links zu weiteren Informationsquellen. Sie haben folgende Möglichkeiten:

- Greifen Sie auf die Online-Virenbibliothek von McAfee zu, um mehr über einen bestimmten Virus herauszufinden.
- Senden Sie eine Virenprobe zur Analyse an McAfee.
- Setzen Sie sich mit dem Technischen Support von McAfee in Verbindung.

Weitere Informationen hierzu finden Sie in der *Online-Hilfe*.

Anhänge

Dieser Abschnitt enthält nützliche Informationen für die Installation und Konfiguration Ihres Blade-Servers.

Inhalt

- Beispiel für die Basiskonfiguration eines Interconnect-Moduls
- Beispiel einer Chassis-Konfigurationsdatei

Beispiel für die Basiskonfiguration eines Interconnect-Moduls

Auf dieser Seite sehen Sie ein Beispiel für die Basiskonfiguration eines der Interconnect-Module eines Blade-Servers, der im ausfallsicheren Modus betrieben wird.

HINWEIS: Für jedes Interconnect-Modul im Blade-Server-Gehäuse ist eine Basiskonfigurationsdatei erforderlich.

Beispiel für die Basiskonfiguration eines Interconnect-Moduls – interconnect_base.*n* (*n* = Interconnect-Modul-Nummer)

```
version "5.1.3"
switch-type "GbE2c L2/L3 Ethernet Blade Switch for HP c-Class BladeSystem"
!
!
!
no system bootp
hostname "sw1"
system idle 60
!
ip dns primary-server 10.9.9.1
!
ntp enable
ntp primary-server 10.9.9.1
ntp interval 60
!
system timezone 180
! Europe/Britain/GB
system daylight
!
!
!
```

access user administrator-password
"ebfec37e832a822ab6b7a2b7409a21d800e2b27007bb4b41b7dd3b7827e7ec0f"
!
!
!
!

Anhänge

Beispiel einer Chassis-Konfigurationsdatei

Auf dieser Seite sehen Sie ein Beispiel für die Chassis-Konfigurationsdatei eines Blade-Servers, der im ausfallsicheren Modus betrieben wird.

Beispiel mit einem Ausschnitt der Datei "chassisconfig.xml" für das Interconnect-Modul mit ID="1"

```
<!-- Copyright (C) 2010 McAfee Inc. All rights reserved. -->

<!-- default configuration layout for EWS usage of the C3000 chassis -->
<!-- this gets merged with the operational requirements based on configuration
-->


<Chassis>
    <Chassis>
        <!-- there are no default credentials since they are different per
chassis -->
        <!-- <OnBoardAdmin username="Administrator" password="password"/> -->

        <!-- the vlan we use for our scanning network -->
        <ScanningVlan vlanTag="4094"/>

        <!-- the vlan we use for external untagged traffic within the chassis --
>
        <UntaggedVlan vlanTag="4093"/>

        <!-- the vlan we use for our OOB network -->
        <OobVlan      vlanTag="4092"/>

        <!-- additional external tagged VLANs that need to be bridged through
from lan1 to lan2 -->
        <!-- <BridgeVlan> <VlanTag vlanTag="1234"/> </BridgeVlan> -->
        <BridgeVlan/>

        <!-- STG definitions for the above -->
        <ScanningSTG id="127" priority="32768" enable="yes"/>
        <ExternalSTG id="1" priority="32767" enable="yes"/>
        <OobSTG id="126" priority="32768" enable="yes"/>
    </Chassis>

    <Networks>
        <!-- the resiliency configuration for the bonded pairs of links -->
        <!-- the lan1/lan2 settings are ignored in transparent bridge mode since
STP is used instead -->
        <!-- we have to automatically calculate the arpTargets for each LAN as
the links are bought up -->
        <Network id="lan1" bond_mode="balance-alb"/>
        <Network id="lan2" bond_mode="balance-alb"/>
        <Network id="scan" bond_mode="balance-alb"/>
        <Network id="oob"  bond_mode="active-backup"/>
```

```
    </Networks>

    <Blades>
        <!-- default topology is that blades 1 and 2 are the management blades
-->
        <Blade id="1" isMgmt="yes"/>
        <Blade id="2" isMgmt="yes"/>
        <!-- this is how to ignore a blade slot completely -->
        <!-- <Blade id="3" ignore="yes"/> -->
    </Blades>

    <Interconnects>
        <Interconnect id="1">
            <!-- Add ip="a.b.c.d" to the credentials node to allow the system to
automatically configure the interconnects -->
            <Credentials username="admin" password="admin" ip="1.2.3.4"/>
            <!-- cross connects -->
            <Ports>
                <!-- Permitted attributes for the Port element are: -->
                <!-- id = the port number -->
                <!-- name = textual label for use in UI and SNMP etc. -->
                <!-- vlanId = 1-4095, the VLAN used for untagged frames on this
port -->
                <!-- enable = yes/no -->
                <!-- edgePort = yes/no, is this an edge port as far as STP is
concerned -->
                <!-- lacpEnable = active/passive/off -->
                <!-- lacpKey = LACP group to identify ports trunked to the same
peer -->
                <!-- lacpPriority = 0-65535, priority for the port within the
LACP group -->
                <!-- stpEnable = yes/no, is STP enabled on this port or not -->
                <!-- ignore = yes/no, if yes then no config will be generated
for this port -->

                <!-- cross connects -->
                <Port id="17" name="CrossConnectAto2" vlanId="defuntagged"
enable="yes" edgePort="no" lacpEnable="active" lacpKey="100" stpEnable="yes"/>
                <Port id="18" name="CrossConnectBto2" vlanId="defuntagged"
enable="yes" edgePort="no" lacpEnable="active" lacpKey="100" stpEnable="yes"/>

                <!-- internal chassis management network port - we can't change
this-->
                <Port id="19" ignore="yes"/>

                <!-- external ports -->
                <Port id="20" name="External20" vlanId="defuntagged"
enable="yes" edgePort="no" lacpEnable="active" lacpKey="101" stpEnable="yes"/>
                <Port id="21" name="External21" vlanId="defuntagged"
enable="yes" edgePort="no" lacpEnable="active" lacpKey="101" stpEnable="yes"/>
                <Port id="22" name="External22" vlanId="defuntagged"
enable="yes" edgePort="no" lacpEnable="active" lacpKey="101" stpEnable="yes"/>
                <Port id="23" name="External23" vlanId="defuntagged"
enable="yes" edgePort="no" lacpEnable="active" lacpKey="101" stpEnable="yes"/>
                <Port id="24" name="External24" vlanId="defuntagged"
```

```
enable="yes" edgePort="no" lacpEnable="active" lacpKey="101" stpEnable="yes"/>
            </Ports>

            <VLANs>
                <!-- Permitted attributes for the VLAN elements are: -->
                <!-- id = 1-4095, VLAN ID -->
                <!-- name = textual name for UI and SNMP etc. use -->
                <!-- stgId = 1-127, spanning tree group for the VLAN -->
                <!-- The ports which are in the VLAN are defined within the VLAN
element -->

                <!-- VLAN for OOB traffic -->
                <!-- blade port bindings are added automatically -->
                <VLAN id="oob"/>

                <!-- VLAN for internal scanning network -->
                <!-- blade port bindings are added automatically -->
                <VLAN id="scan">
                    <Port id="17"/>
                    <Port id="18"/>
                </VLAN>

                <!-- VLAN(s) for external traffic -->
                <!-- blade port bindings are added automatically -->
                <VLAN id="external" stgId="1">
                    <Port id="17"/>
                    <Port id="18"/>
                    <Port id="20"/>
                    <Port id="21"/>
                    <Port id="22"/>
                    <Port id="23"/>
                    <Port id="24"/>
                </VLAN>
            </VLANs>

        </Interconnect>

    </Interconnects>


</Chassis>
```

▸ Anhänge

Prozeduren für den Hardwareaustausch

Gehen Sie folgendermaßen vor, um fehlerhafte Hardwarekomponenten auszutauschen.

Vorgehensweise

▸ Anhänge
▸ Ersetzen eines ausgefallenen Scan-Blades
▸ Ersetzen eines ausgefallenen Management-Blade-Servers
▸ Ersetzen eines ausgefallenen Failover-Management-Blade-Servers
▸ Ersetzen eines ausgefallenen Interconnect-Moduls
▸ Ersetzen eines ausgefallenen Onboard-Administrator-Moduls

Ersetzen eines ausgefallenen Scan-Blades

Gehen Sie wie nachfolgend beschrieben vor, um ein ausgefallenes Scan-Blade zu ersetzen.

Falls das neue Blade leere Festplatten hat, wird automatisch ein Scan-Blade-Image installiert. Gehen Sie anderenfalls wie unter Installieren der Software auf einem Blade-Server zum Scannen von Inhalten beschrieben vor, um eine Neuinstallation der Software auf dem Scan-Blade zu erzwingen.

Vorgehensweise

1. Fahren Sie das Blade herunter.
   Warten Sie darauf, dass sich das Blade ausschaltet.
2. Ersetzen Sie das Blade, nachdem es sich ausgeschaltet hat.

Ersetzen eines ausgefallenen Management-Blade-Servers

Gehen Sie wie nachfolgend beschrieben vor, um einen ausgefallenen Management-Blade-Server zu ersetzen.

Vorgehensweise

1. Fahren Sie den Management-Blade-Server herunter.
2. Entfernen Sie den alten Management-Blade-Server.
3. Setzen Sie den neuen Management-Blade-Server ein.
4. Installieren Sie die EWS-Software. Weitere Informationen über die Neuinstallation der Software und die Konfiguration des Management-Blade-Servers finden Sie unter Installieren der Software.
5. Konfigurieren Sie das neue Blade als Management-Blade-Server (sofern erforderlich).

Ersetzen eines ausgefallenen Failover-Management-Blade-Servers

Gehen Sie wie nachfolgend beschrieben vor, um einen ausgefallenen Failover-Management-Blade-Server zu ersetzen.

Vorgehensweise

1. Fahren Sie den Failover-Management-Blade-Server herunter.
2. Entfernen Sie den alten Failover-Management-Blade-Server.
3. Setzen Sie den neuen Failover-Management-Blade-Server ein.
4. Installieren Sie die EWS-Software. Weitere Informationen über die Neuinstallation der Software und die Konfiguration des Failover-Management-Blade-Servers finden Sie unter Installieren der Software.
5. Konfigurieren Sie das neue Blade als Failover-Management-Blade-Server (sofern erforderlich).

Ersetzen eines ausgefallenen Interconnect-Moduls

Gehen Sie wie nachfolgend beschrieben vor, um ein ausgefallenes Interconnect-Modul zu ersetzen.

Zum Ersetzen eines ausgefallenen Interconnect-Moduls ist es erforderlich, entweder eine Systemstillstandszeit einzuplanen, um das Ersatz-Interconnect-Modul vor Ort zu konfigurieren, oder das Interconnect-Modul in einem zweiten Blade-Server getrennt vom Produktionssystem zu konfigurieren. Das Ersatz-Interconnect-Modul muss offline konfiguriert werden, da die Standardkonfiguration die laufende Netzwerktopologie beeinträchtigen könnte.

So ersetzen Sie ein Interconnect-Modul, wenn kein Reserve-Blade-Server verfügbar ist:

Vorgehensweise

1. Fahren Sie alle Scan-Blades herunter.
2. Fahren Sie den Failover-Management-Blade-Server herunter.
3. Laden Sie die Konfigurationsdatei für das Interconnect-Modul vom Management-Blade-Server herunter (falls die EWS-Software das Interconnect-Modul nicht automatisch konfigurieren darf).
4. Trennen Sie das Chassis von allen Netzwerken mit Ausnahme des OOB-Netzwerks (wenn Sie die Interconnect-Module 1 oder 2 ersetzen) oder des LAN1-Netzwerks (wenn Sie die Interconnect-Module 3 oder 4 ersetzen), so dass nur noch ein Interconnect-Modul mit dem verbleibenden LAN verbunden ist.
5. Ersetzen Sie das Interconnect-Modul, und schalten Sie es ein.
6. Stellen Sie sicher, dass das Interconnect-Modul eine geeignete IP-Adresse. Dies sollte automatisch der Fall sein, wenn das Interconnect-Modul seine IP-Adresse über DHCP und das OA-Modul bezieht.
7. Wenn die EWS-Software das Interconnect-Modul nicht automatisch konfigurieren darf, laden Sie die Konfiguration des Interconnect-Moduls hoch. Wenn die EWS-Software das Interconnect-Modul automatisch konfigurieren darf, verwenden Sie die Schaltfläche "Interconnect-Modul-Konfiguration übernehmen" der grafischen EWS-Benutzeroberfläche EWS GUI, oder geben Sie in der Textkonsole des Konsoles folgenden Befehl ein: scm /opt/NETAwss/resiliency/apply_chassis_config
8. Verifizieren Sie, dass das Interconnect-Modul die Konfiguration ohne Fehler angenommen hat.
9. Stellen Sie die Netzwerkverbindungen wieder her.
10. Schalten Sie den Failover-Blade-Server und die Scan-Blades wieder ein.

Ersetzen eines ausgefallenen Onboard-Administrator-Moduls

Die korrekte Vorgehensweise beim Austausch des Onboard-Administrator-Moduls finden Sie in der HP-Dokumentation.

Index

A

Anhänge, E-Mail ist blockiert 96
Antiviren-Aktualisierungen, nichts geschieht 95

B

Basiskonfigurationen
  Erstellen 83
  Interconnect-Modul 83
Basiskonfigurationen für Interconnect-Module
  Erstellen 83
Berichte
  Generieren 62
Berichterstellung 62
Blade-Server
  Installieren 31
  Verbinden 31

D

Directory Harvest-Prävention funktioniert nicht 99
Directory Harvest-Prävention, funktioniert nicht 96

E

E-Mail-Replikation funktioniert nicht 99
E-Mail-Verkehr
  Testen 69
E-Mails, alle blockiert 96
E-Mails, durch Anhänge blockiert 96
E-Mails, gesperrt als Spam 93
EICAR-Testvirus, E-Mail gelangt durch 97
Erforderliche Informationen 27, 77
Erstellen der Basiskonfigurationen für Interconnect-Module 83

F

Fehlerbehebung, Einführung in 91
FTP, Hochladen über HTTP 92
FTP, in Browsern 92

H

Hardware-Informationen 77
Häufig gestellte Fragen 91
Häufig gestellte Fragen, ICAP 97
HotFix, nicht akzeptiert 101
HTTP, kein Hochladen über HTTP 92

I

ICAP, häufig gestellte Fragen 97
Informationen
  Erforderlich 27, 77
  Hardware 77
Installieren
  Blade-Server 31
Interconnect-Module
  Umkonfigurieren von einer früheren Version 32

K

Konfiguration
  Sichern 33, 80
Konfiguration sichern 33, 80

L

Lotus Domino 99

M

Mail, Zustellprobleme 96
Microsoft Exchange-Server, ESMTP-Problem 99

N

Netzteil
  Verbinden 39

P

POP3 funktioniert nicht 100
POP3, zwei Mail-Kopien 100
Posteingänge sind voll 95
Probleme, Schaltfläche "Zurück" 100
Protokolle, Größe steuern 101

Q

Qmail, Microsoft Exchange 2000 und 2003 99

S

Spam, Benutzer erhalten weiterhin 94
Spam, keine normale E-Mail kommt durch 93
Spam, kommt trotz RBL durch 93
Spam, Stoppen eines Typs 95
Spam, volle Posteingänge 95
Stromversorgung 39

T

Testen
  Virenerkennung 69
Testen des E-Mail-Verkehrs 69

V

Verbinden
  Blade-Server 31
Virus verursacht Inhaltsverletzung 97

Z

Zurück, Problem mit Schaltfläche 100
Zustellung 96

700-2816B15

McAfee®